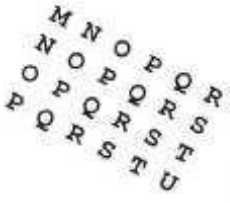
Wer knackt den Code?



A	B	C	D	E	F	G	H	I	J	K	L														
B	C	D	E	F	G	H	I	J	K	L	M														
C	D	E	F	G	H	I	J	K	L	M	N														
D	E	F	G	H	I	J	K	L	M	N	O														
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V								
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W								
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X								
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y								
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z								
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A								
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B								
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C								
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D								
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E								

1. Wer knackt den Code?
Eine Unterrichtssequenz zur Stochastik in Klasse 7/8

1.1 Bemerkungen zur Kryptographie

Der Wunsch nach Geheimhaltung wichtiger Nachrichten ist so alt wie die Menschheit selbst. Vertrauliche Informationen soll nur der eigentliche Empfänger erhalten, gelangen geheime Botschaften dagegen in die falschen Hände, so kann dies seit jeher schwerwiegende Folgen haben. Diese Gefahr war und ist der eigentliche Ansporn für die Entwicklung von Verschlüsselungstechniken.
Professionell beschäftigten sich Jahrhunderte lang hauptsächlich Militärs mit kryptologischen Fragestellungen. Rivalisierende Staaten richteten Verschlüsselungsdienste ein, um Nachrichten möglichst sicher transportieren zu können. Gleichzeitig versuchten sie gegnerische Codes zu entschlüsseln und auf diese Weise Geheimnisse zu stehlen. Die verwendeten Codes haben zahlreiche Schlachten beeinflusst und vielfach über Leben und Tod entschieden. So ist die Geschichte der Kryptographie eine Geschichte vom unablässigen Kampf zwischen Verschlüsslern und Entschlüsslern, die jeweils nach einer Verbesserung ihrer Verfahren trachteten.
Die ständigen Angriffe der Codebrecher und die Entwicklung neuer Codierungsverfahren haben zu einer ganzen Reihe bemerkenswerter wissenschaftlicher Durchbrüche geführt. Beispielhaft sei hier nur auf die Verbindung zwischen kryptoanalytischen Attacken und der Entwicklung des modernen Computers verwiesen. Für die Ver- und Entschlüsselung von Nachrichten wurden zunehmend Methoden der Mathematik und Linguistik, der Informatik und Quantentheorie angewendet, die Erkenntnisse der Kryptologen führten umgekehrt zu einer Bereicherung dieser Fachgebiete.
Seit der überwältigenden Verbreitung der elektronischen Datenverarbeitung seit den 60er Jahren gewinnt die Auseinandersetzung mit Fragen der Datensicherheit verstärkt an Bedeutung. Die Kommunikationsrevolution hat die Gesellschaft verändert, Information wird zu einer immer wertvolleren Ware, die es zu schützen gilt.
Die Kryptologie ist daher heute bedeutsamer denn je, ständig wird sie vor neue Aufgaben gestellt. Neben die klassischen militärischen Anwendungen sind zahlreiche Anforderungen aus dem privaten und geschäftlichen Bereich getreten. Die Übermittlung von Telefongesprächen über Satellit, das Verschicken elektronischer Post, Pay-TV, Homebanking, der Einsatz von Chipkarten oder Probleme mit Computerviren seien hier als Beispiele für die neuen Herausforderungen genannt. Wird es gelingen, hier absolut sichere Verfahren zu entwickeln oder werden die Codebrecher den Sieg davontragen? Der Computer spielt dabei eine besondere Rolle. Er ist die Ursache für zahlreiche Probleme mit der Datensicherheit und zugleich Mittel zu ihrer Lösung.
Als Kunst der geheimen Kommunikation wird die Kryptographie jedenfalls die Schlösser und die Schlüssel des Informationszeitalters bereitstellen.

1.2 Geheimschriften im Mathematikunterricht

Gerade weil die Kryptographie eine hochaktuelle Wissenschaft ist und bei der Ver- und Entschlüsselung von Daten mit mathematischen Methoden operiert, bietet sich eine Behandlung von Geheimschriften im Mathematikunterricht unbedingt an. Auf fast spielerische und zunächst wenig mathematisch scheinende Weise können die

Schülerinnen und Schüler an die Grundprinzipien der Kryptographie herangeführt werden, wobei sie schnell lernen handfest zu argumentieren.
Der konkrete Unterricht sollte die drei Grundmotive der Kryptologie ständig im Auge behalten: das Verschlüsseln einer Nachricht durch den Sender, das Entschlüsseln der Botschaft durch den eigentlichen Empfänger und das „Knacken" eines geheimen durch einen Codebrecher (Angreifer). Die Schülerinnen und Schüler können in die entsprechenden Rollen schlüpfen, gerade als Codebrecher dürften sie besonders motiviert sein.
Schon in den Klassen 5 und 6 lassen sich einfache Geheimschriften (z. B. Verschlüsselungen mit der Skytale von Sparta, der Übersetzung von Buchstaben in Zahlen verschiedener Stellenwertsysteme, dem Polybios-Code, der Gartenzaun-Methode oder etwa mit Schablonen) an verschiedenen Stellen gut in den Mathematikunterricht integrieren. Entsprechende Hinweise und Beispiele sind der angegebenen Literatur oder dem Internet leicht zu entnehmen. Auch eigene Geheimschriften der Kinder können hier ausprobiert und ggf. vorläufig schon auf ihre Sicherheit hin untersucht werden.
Die vorliegende Unterrichtssequenz ist für den Anfangsunterricht in Stochastik in den Klassen 7 und 8 geeignet. An mehreren Beispielen aus der Geschichte der Kryptographie sammeln die Schülerinnen und Schüler dabei Erfahrungen mit einigen, für die Statistik wichtigen Begriffen wie Strichliste, Rangliste, absolute und relative Häufigkeiten. Typische Verfahren der Statistik werden hier angewendet und eingeübt: Die Erhebung von Daten etwa beim Zählen bestimmter Geheimtextbuchstaben zu Beginn einer Kryptoanalyse findet ebenso Berücksichtigung wie deren Darstellung in Häufigkeitstabellen und Diagrammen. Beim endgültigen Brechen der Codes spielt vor allem die Beschreibung und Interpretation der veranschaulichten Daten eine besondere Rolle.

1.3 Lernziele

Neben das Anwenden und Einüben statistischer Grundbegriffe und Verfahren tritt bei der vorliegenden Unterrichtssequenz das Erlernen kryptographischer Grundprinzipien. Die Schülerinnen und Schüler sollen wichtige Meilensteine aus der Geschichte der Kryptographie kennenlernen und die Vor- und Nachteile der einzelnen Verschlüsselungsverfahren angemessen beschreiben können. Auch sollen sie um die wachsende Bedeutsamkeit dieser Disziplin wissen. Beim „Knacken" von Geheimschriften sollen die Schülerinnen und Schüler statistische Methoden angemessen anwenden Können und dabei im Umgang mit dem Computer bzw. Taschenrechner sicherer werden.
Zudem zielt die Reihe auf eine Förderung des eigenverantwortlichen Lernens und die Entwicklung von Teamfähigkeit.

1.4 Hinweise zum Einsatz der Materialien im Unterricht

Zu Beginn der Unterrichtssequenz können die Schülerinnen und Schüler mit dem Text „Geheime Botschaften" vielleicht in einer vorbereitenden Hausaufgabe für die neue Thematik sensibilisiert werden. Alternativ kann hier von der Lehrerin bzw. dem Lehrer oder besser noch von einer Schülerin oder einem Schüler ein kurzes Impulsreferat über Kryptographie gehalten werden; dies setzt allerdings genügend Vorbereitungszeit voraus.

Da man beim Thema Geheimschriften kaum auf wesentliche Begriffe und übliche Vereinbarungen verzichten wird, kann zu Beginn der Lerneinheit an einer passenden Stelle auch das nachfolgende Puzzle eingesetzt und ggf. zur Lernkontrolle in ein Kreuzworträtsel überführt werden.
Das Arbeitsblatt „Geheimschrift von Julius Caesar" dient der Einführung einer Verschiebechiffre, der Text sollte zunächst in Einzelarbeit von den Schülerinnen und Schülern erschlossen werden. Die abschließende Aufgabe dient der Ergebnissicherung und ist für eine Partnerarbeit gedacht.
In der zweiten Unterrichtsstunde geht es um beliebige Caesar-Verschiebungen und das Basteln von Caesar-Scheiben. Der Text auf dem gleichnamigen Arbeitsblatt kann in der Klasse von einigen Schülerinnen und Schülern vorgelesen und dann gemeinsam besprochen werden. Auf das anschließende Basteln eigener Caesar-Scheiben sollte auf keinen Fall verzichtet werden, zumal diese auch im weiteren Verlauf der Reihe immer wieder verwendet werden können. Die beiden Bastelanleitungen können je nach Vorwissen alternativ oder zur Binnendifferenzierung auch beide für unterschiedliche Schülergruppen eingesetzt werden. Bei der ersten wird nur die Konstruktion eines Kreismittelpunktes bei vorgegebenem Kreisrand (etwa mit Hilfe des Schnittpunkts der Mittelsenkrechten zweier Sehnen) wiederholt. Die zweite Bastelanleitung macht das Zeichnen von Winkeln und das Arbeiten mit Näherungswerten erforderlich. Verschiedentlich wurde vorgeschlagen, die Anzahl der Kreisausschnitte zur Vereinfachung auf 36 zu erhöhen, indem auch Satzzeichen und Umlaute berücksichtigt werden, dies führt aber bei der Häufigkeitsanalyse von Geheimtexten später zu Schwierigkeiten. Entlang der Aufgaben 2 bis 4 können die Caesar-Scheiben dann ausprobiert werden. Bei der letzten Aufgabe ist Vorsicht geboten: Die Lösung verspricht den Schülerinnen und Schülern einen Nachmittag ohne Hausaufgaben in Mathematik!
Die nächste Unterrichtsstunde, die mit einer kurzen Wiederholungsphase beginnen sollte, führt entlang des Arbeitsblatts „Das häufige e und das seltene q" zum Einstieg in die Häufigkeitsanalyse. Die von den Schülerinnen und Schülern in Stillarbeit produzierten Sätze zur ersten Aufgabe können im Plenum vorgelesen und ggf. in einer besonderen Form honoriert werden. Die vier Teile der zweiten Aufgabe können wiederum in Einzel-, aber auch in Partnerarbeit oder teilweise als Hausaufgabe gelöst werden. Je nach Leistungsstand der Klasse sind hier ggf. Hilfestellungen für einzelne Schülerinnen und Schüler erforderlich.
Um die Beschränkung auf 25 Geheimalphabete aufzuheben, wird im weiteren Verlauf der Unterrichtssequenz mit beliebigen monoalphabetischen und später auch mit polyalphabetischen Zuordnungen gearbeitet. Zum „Knacken" solcher Geheimschriften benötigt man dringend eine Häufigkeitsverteilung der Buchstaben des deutschen Alphabets, die in der vierten und fünften Stunde aufgestellt und auf besondere Merk- male hin untersucht wird. Entlang der Arbeitsblätter „Wir zählen Buchstaben" werten die Schülerinnen und Schüler zunächst genau 400 Buchstaben eines recht zufällig ausgewählten Textes aus und berechnen für jeden Buchstaben zu den absoluten auch die relativen Häufigkeiten. Die einzelnen Ergebnisse werden anschließend erst in kleinen Gruppen und dann auch für die gesamte Klasse zusammengefasst. Auf diese Weise kann der hypothetische Charakter des Wahrscheinlichkeitsbegriffs gut vorbereitet werden. Die entscheidende Frage lautet doch, mit welcher Wahrscheinlichkeit ein beliebig aus einem deutschen Text herausgezogener Buchstabe etwa der Buchstabe a ist. Wahrscheinlichkeiten werden so zu Prognosen, um die die relativen Häufigkeiten der zu einem Geheimtext gehörenden Klartextbuchstaben schwanken werden. Die relativen Häufigkeiten, die von der gesamten Klasse ermittelt wurden, werden also so lange als Wahrscheinlichkeiten verwendet, bis eine größere Stich-

probe notwendig wird und zu noch genaueren Werten führt. Aus diesem Grund ist es auch nicht sinnvoll, den Schülerinnen und Schülern die Werte von A. Beutelspacher aus der Lehrerlösung als endgültige und exakte Werte zu präsentieren; die Klassenergebnisse sind für die weiteren Untersuchungen sicherlich völlig ausreichend.

Zur Erstellung der Tabellen und bei der Lösung der anschließenden Aufgaben bietet sich der Computereinsatz unbedingt an (vgl. die Ausführungen unten). Dem Balkendiagramm (Aufgabe 1) kommt eine besondere Bedeutung zu, da es zusammen mit der Rangliste (Aufgabe 4) als entscheidende Interpretationshilfe beim „Knacken" komplexerer Geheimschriften Verwendung finden wird. Mit dem Balkendiagramm lässt sich wegen der größeren Anschaulichkeit besser arbeiten als mit der (unsortierten) Tabelle der relativen Häufigkeiten. Die besonderen Merkmale der Häufigkeitsverteilung der Buchstaben (Aufgabe 3) sind hier leicht zu erkennen. Ein Vergleich mit dem letzten Balkendiagramm (Aufgabe 2) zeigt, dass die normale Häufigkeitsverteilung der Buchstaben bei Caesar-Verschiebungen erhalten bleibt, sie ist nur verschoben. Die Klasseneinteilung (Aufgabe 5) führt zu einem anderen Diagrammtyp, die verschiedenen Schülerergebnisse sollten im Unterrichtsgespräch erörtert werden. So zeigt das Kreisdiagramm in der Lehrerlösung, dass ein „normaler deutscher Text" zu ca. 62% aus nur sieben Buchstaben besteht. Dagegen machen die sechs seltensten Buchstaben nur 2% eines solchen Textes aus.

In der sechsten und siebten Stunde der Unterreihe geht es um die Kryptoanalyse monoalphabetischer Schlüsselwortchiffrierungen. Die Arbeitsblätter „Caesar mit Schlüsselwort" eignen sich zum selbsttätigen Arbeiten der Schülerinnen und Schüler.

Für die ersten drei kleinen Aufgaben sollte die Lehrerin bzw. der Lehrer entsprechende Kontrollkarten mit den Lösungen zur Verfügung stellen. Die letzte Aufgabe dient der Anwendung des zuvor beschriebenen Verfahrens. Da der Text länger und die Kryptoanalyse dementsprechend etwas zeitaufwändiger ist, kann hier gut in Partner oder arbeitsteiliger Gruppenarbeit vorgegangen werden.

Im Sinne einer Ergebnissicherung ist es nun an der Zeit Rückschau zu halten. Im Unterrichtsgespräch sollten die Schülerinnen und Schüler sämtliche Caesar-Verfahren, ihre Nachteile und die Methoden zum „Knacken" der Geheimschriften beschreiben, um den Blick für die ständige Auseinandersetzung zwischen Verschlüsslern und Codebrechern zu schärfen. Abschließend können sie Optionen für eine „optimalere" Geheimschrift zusammentragen.

In den letzten Unterrichtsstunden der Reihe erarbeiten die Schülerinnen und Schüler das Vigenère-Verfahren als wohl bekannteste Form einer polyalphabetischen Verschlüsselung. Den Text der ersten Arbeitsblätter („Vigenère-Verschlüsselung") sollten sich die Kinder erneut selbstständig erschließen. Bei den zugehörigen Aufgaben muss darauf geachtet werden, dass der Zusammenhang zwischen dem Vigenère-Verfahren und der Verwendung der Caesar-Scheiben (Aufgabe 2) deutlich erkannt wird, da dieser einen Schlüssel zum Brechen solcher Codes darstellt. Die statistische Untersuchung des Geheimtextes zu Aufgabe 3 lässt den großen Vorteil dieser Verschlüsselungsmethode sichtbar werden. Nähere Erläuterungen hierzu sind der Lehrerlösung zu entnehmen.

Beim „Knacken" Vigenère-verschlüsselter Texte ist man gut beraten, wenn man die Länge des Schlüsselworts zunächst als bekannt voraussetzt. Der zweite Teil des Kasiski -Tests bereitet dann keine großen Schwierigkeiten, er kann mit Hilfe der bereits eingeübten Verfahren gelöst werden. Die für die drei Teiltexte jeweils erforderliche Häufigkeitsanalyse kann daher in arbeitsteiliger Gruppenarbeit mit dem beigefügten Arbeitsblatt („Gruppenarbeit Vigenère") durchgeführt werden. Die im Materialteil genauer beschriebene Methode Jigsaw bietet sich dabei an.

Um im ersten Teil des Kasiski-Tests die Länge des Schlüsselworts zu berechnen, bedarf es des Rückgriffs auf die Teilbarkeitslehre in Klasse 6. Je nach Vorwissen der Schülerinnen und Schüler muss zunächst gemeinsam geklärt werden, was man unter dem Abstand zweier Buchstabenfolgen versteht. Ggf. ist an weiteren Beispielen auch der Zusammenhang zwischen der Schlüsselwortlänge und dem ggT der Abstände gleicher Buchstabenfolgen breiter als auf dem Arbeitsblatt zu erklären. Die Unterrichtsreihe endet mit einem Ausblick auf das One time pad, einem absolut sicheren Verschlüsselungssystem.

1.5 Aufgabenkultur, Vernetzung, Arbeitstechniken, Hinweise zu Klassenarbeiten

Im Rahmen der Unterrichtssequenz „Wer knackt den Code?" werden die zuvor im Unterricht erarbeiteten statistischen Grundbegriffe und Verfahren an Beispielen aus der Kryptographie angewendet und eingeübt. Die Geheimschriften stellen dabei einen abwechslungsreichen, komplexen und bedeutsamen mathematikhaltigen Kontext dar, aus dem die einzelnen Aufgaben hergeleitet werden. Gerade bei der Kryptoanalyse monoalphabetischer Schlüsselwortchiffrierungen und Vigenère-chiffrierter Texte wird das Erheben, Darstellen und Interpretieren von Daten sinnvoll miteinander verknüpft, um den Geheimtext in den zugehörigen Klartext zu überführen. Das Üben kann für die Schülerinnen und Schüler auf diese Weise an Reiz und Bedeutung gewinnen und zu einer Konsolidierung des Wissens beitragen.
Aufgrund der Komplexität des Themas dienen die einzelnen Aufgabenstellungen in den Materialien zunächst dem Ziel, die Schülerinnen und Schüler mit den Ver- und Entschlüsselungstechniken vertraut zu machen. Bestimmte Verfahren der Kryptographie müssen hier gesichert und automatisiert werden, die Mathematik kommt dabei von ganz alleine zu ihrem Recht. Beim endgültigen Knacken von Geheimtexten durch eine Bewertung der durch Kryptoanalyse gewonnenen Daten kann dagegen nicht mehr rein schematisch gearbeitet werden. Hier geht es um wirklich anspruchs- volle Denk- und Übertragungsprobleme und den Erwerb flexiblen Wissens. Unter- schiedliche Lösungswege bieten sich an und können im Unterricht miteinander verglichen werden.
Auf die thematische Vernetzung wurde oben bereits hingewiesen. Einfache Geheimschriften lassen sich in den Lernbereichen Algebra und Geometrie problemlos schon in den Klassen 5 und 6 behandeln. Die Unterschiede zwischen mono- und polyalphabetischen Verschlüsselungen und die entsprechenden Konsequenzen, die sich aus dem Verzicht auf Eindeutigkeit etwa beim Verfahren von Vigenère ergeben, können später bei einer Unterrichtsreihe über Zuordnungen und Funktionen wieder aufgegriffen und von einem höheren Standpunkt aus vertiefend erörtert werden. In der gymnasialen Oberstufe bietet sich das Thema Codierung und Decodierung bei der Einführung der inversen Matrix an.
Die vorliegende Unterrichtssequenz ermöglicht zudem ein Wiederholen auch länger zurückliegender Stoffe. Dies reicht von der Konstruktion eines Kreismittelpunktes und dem Zeichnen von Winkeln und Arbeiten mit Näherungswerten beim Basteln der Caesar-Scheiben über Zähltechniken und die Berechnung von Prozentsätzen bis zur Anwendung der Teilbarkeitslehre bei der Bestimmung der Schlüsselwortlänge zum „Knacken" Vigenère-verschlüsselter Texte.

Es ist nicht sinnvoll, beim Anwenden und Einüben statistischer Grundbegriffe und Verfahren auf mathematikhaltige Kontexte wie die Geheimschriften zu setzen und bei

der Leistungsüberprüfung alles beim Alten zu belassen. Bei den Klassenarbeiten sollten daher vor allem die Caesar-Chiffren Berücksichtigung finden. Die Caesar- Scheiben können als Hilfsmittel problemlos zugelassen werden. Neben der Ver- und Entschlüsselung vorgegebener Texte kann hier auch das Erstellen oder Auswerten von Häufigkeitstabellen und Diagrammen eine Rolle spielen. Bei leistungsstärkeren Klassen besteht sogar die Möglichkeit, die Schlüsselwortlänge eines Vigenère-verschlüsselten Textes mit dem Kasiski-Test berechnen und mit Hilfe einer Häufigkeitsanalyse etwa zum ersten Schlüsselwortbuchstaben auch den zugehörigen Klartextbuchstaben bestimmen zu lassen.

Folgende Arbeitstechniken sind im Verlauf der Reihe von Bedeutung:

- wesentliche Informationen aus (mathematischen) Texten erschließen
- Arbeitsschritte bzw. Lösungswege planen
- statistische Daten erheben, analysieren und bewerten
- Schätzen und Überschlagen
- logisches Argumentieren unter Rückgriff auf mathematische Begriffe und Verfahren
- Umgang mit Geodreieck, Zirkel und Lineal
- verständiger Umgang mit dem Taschenrechner und Computer
- Arbeitsergebnisse präsentieren

Auch wenn man anfangs wohl kaum auf die Arbeit mit Geodreieck, Zirkel, Lineal und dem Taschenrechner verzichten wird, ist der Einsatz des Computers im weiteren Fortgang der Reihe zur Motivation der Schülerinnen und Schüler und auch aus zeitökonomischen Gründen sicherlich sinnvoll. Mit einer Tabellenkalkulation lassen sich Häufigkeits- und Verschlüsselungstabellen leicht erstellen, die zugehörigen Kreis- und Balkendiagramme zeichnen, Tabellen einfach zu Ranglisten sortieren und relative Häufigkeiten und der ggT der Abstände schnell berechnen. Der Einsatz eines Textverarbeitungsprogramms bietet sich zum Einscannen eines Textes, zum Zählen sämtlicher Buchstaben (z. B. in Word mit der Funktion „Wörter zählen") oder auch nur bestimmter Buchstaben eines Textes (mit der Funktion „Ersetzen"), zum Erstellen eines Vigenère-Quadrats, dem Ermitteln gleicher Buchstabenfolgen (mit der Funktion „Suchen") sowie zum Ver- und Entschlüsseln kurzer Texte (wieder mit der Funktion „Ersetzen") an.
Die Schülerinnen und Schüler sollten sich die längeren Informationstexte grundsätzlich möglichst selbstständig erschließen. Im Sinne des eigenverantwortlichen Arbeitens sollten sie zudem aufgefordert werden, auch mit eigenen Klar- und Geheimtexten zu experimentieren, weitere Informationen zur Kryptographie zu sammeln und in den Unterricht einzubringen. Kurzreferate sind zu zahlreichen Themen (Kryptographie, Enigma, Caesar, Vigenère, Babbage usw.) möglich, das Internet kann hier sinnvoll für Recherchen genutzt werden.

1.6 Literaturliste:

Bauer, F. L.,	Entzifferte Geheimnisse (Berlin u.a. 1995).
Bertrand, K.,	Wer knackt den Code? : Geolino (4/1999) 16-22.
Beutelspacher, A.,	Kryptologie. Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen (Braunschweig, Wiesbaden [5] 1996).
Beutelspacher, A.,	Mathe-Welt Geheimschriften : Mathematik lehren 72 (Velber 1995).
Franke, H. W.,	Die geheime Nachricht (Frankfurt a.M. 1982).
Kippenhahn, R.,	Verschlüsselte Botschaften. Geheimschrift, Enigma und Chipkarte (Hamburg 1997).
Singh, S.,	Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet (München, Wien 2000).

1.7 Materialien

1. Geheime Botschaften - Text zur Sensibilisierung der Schülerinnen und Schüler
2. Wichtige Begriffe - Puzzle mit Lösung
3. Geheimschrift von Julius Caesar - Arbeitsblatt zur Einführung einer Verschiebechiffre
4. Caesar-Scheiben - Arbeitsblatt zu Verschiebechiffren
5. Bastelanleitungen für Caesar-Scheiben
6. Das häufige e und das seltene q - Arbeitsblatt zum Einstieg in die Häufigkeitsanalyse mit Lösungen
7. Wir zählen Buchstaben - Arbeitsblätter zur Häufigkeitsverteilung der Buchstaben des deutschen Alphabets mit Lösungen
8. Caesar mit Schlüsselwort - Arbeitsblätter zur Kryptoanalyse monoalphabetischer Schlüsselwortchiffrierungen mit Lösung
9. Vigenère-Verschlüsselung - Arbeitsblätter zum Einstieg in polyalphabetische Verschlüsselungen mit Lösung
10. Wir knacken Vigenère - Arbeitsblätter zur Kryptoanalyse Vigenère-chiffrierter Texte (Kasiski-Test)
11. Arbeitsblatt zur Gruppenarbeit bei der Vigenère-Entschlüsselung
12. Methode Jigsaw/Gruppenpuzzle - Kurzübersicht
13. Wir knacken Vigenére - Lösungen zur Gruppenarbeit

Geheime Botschaften

Vielleicht hast du schon einmal mit Geheimtinte, etwa aus Zitronensaft, eine geheime Botschaft an einen Freund oder eine Freundin geschrieben. Oder, du hast von der „Räubersprache“ bei Kalle Blomquist gelesen, die den Mitgliedern der „Weißen Rose“ das Leben rettet.

Du kennst sicher die Abkürzung „lol“ vom Simsen oder Chatten. Aber verstehst du auch „555“? In Thailand spricht man „5“ wie „ha“ aus. Du kennst jetzt den „Schlüssel“ („5“ entspricht „ha“) zum Entschlüsseln von „555“.
Wenn du den Schlüssel kennst, kannst du den „Geheimtext“ lesen, ohne den Schlüssel bleibt dir die Botschaft „555“ ein Rätsel.

Seit Jahrtausenden befassen sich die Menschen mit dem Verschlüsseln von Botschaften. Insbesondere war und ist dies in Kriegszeiten wichtig. Eine bedeutende Rolle spielt etwa die berühmte Caesar-Verschlüsselung, die Julius Caesar vor ca. 2000 Jahren zum Austausch von Botschaften mit seinen Soldaten nutzte. Aber schon 400 Jahre zuvor wusste der Spartanerkönig Leonidas vom bevorstehenden Angriff des persischen Königs Xerxes durch eine auf einem Wachstäfelchen verborgene Botschaft.

Noch heute gilt die moderne Technik der Verschlüsselung in einigen Ländern als Kriegswaffe und die Verbreitung dieser Technik ist dort strafbar.

In allen Zeiten versuchten Herrscher stets die geheimen Nachrichten ihrer Feinde abzufangen und zu entschlüsseln. In sogenannten „Schwarzen Kammern“ waren Spezialisten damit beauftragt, die Schlüssel zum Lesen der Botschaften zu finden. Im Erfolgsfall konnte dies tödliche Folgen haben: Die schottische Königin Maria Stuart wurde in London von der englischen Königin Elisabeth I gefangen gehalten. Als man eine ihrer aus dem Gefängnis geschmuggelten Geheimnachrichten entschlüsselt hatte, wurde sie aufgrund dieser Nachricht geköpft.

Berühmt ist in diesem Zusammenhang die Geschichte der ENIGMA, einer von den Deutschen während des Zweiten Weltkriegs genutzten Verschlüsselungsmaschine. Diese hielt man für praktisch unknackbar. Allerdings gelang es einer englischen Gruppe von Mathematikern den Schlüssel zu finden. So konnten die Geheimnachrichten der Deutschen von den Kriegsgegnern mitgelesen werden.

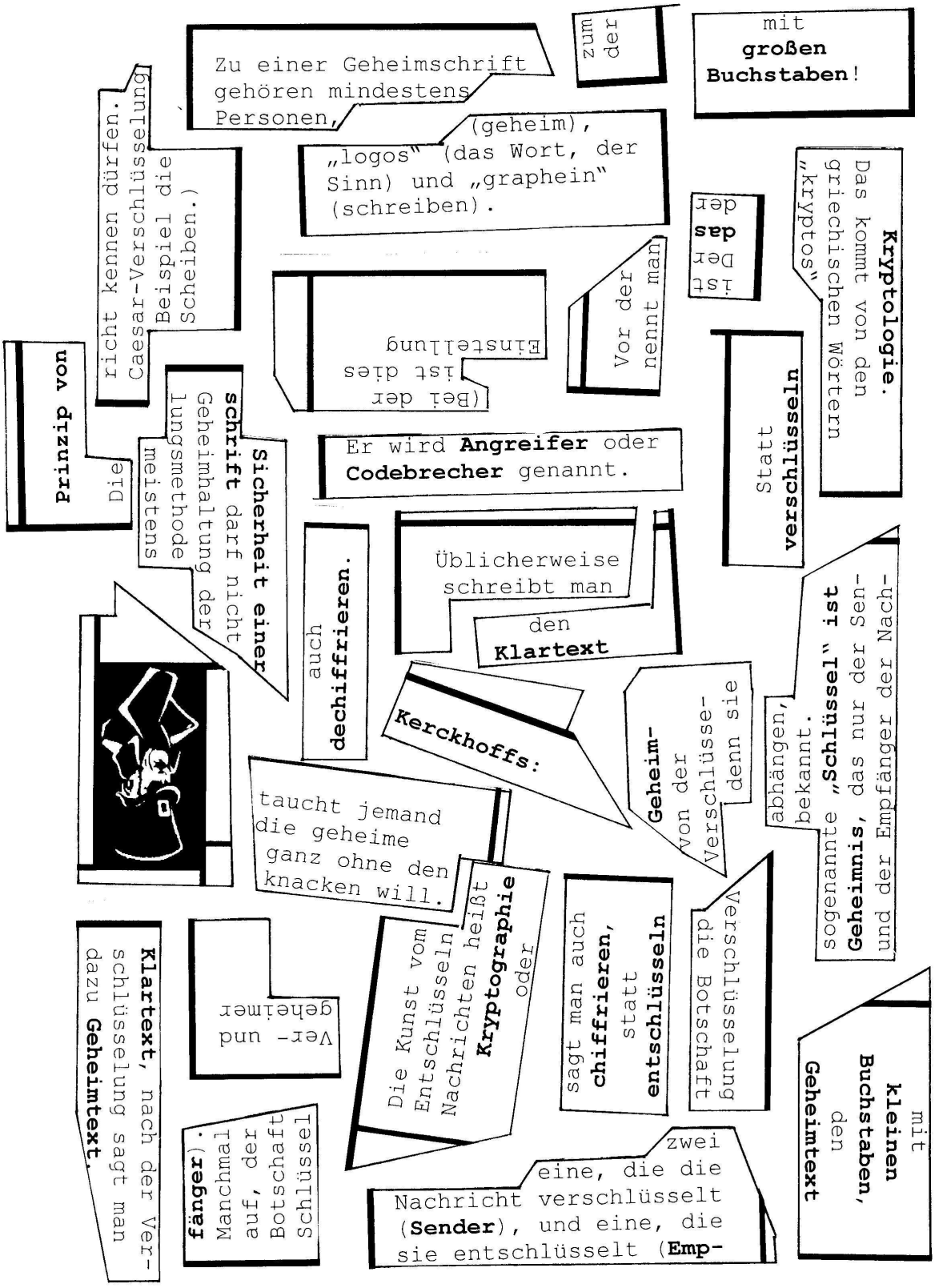
Heute gehört Verschlüsselungstechnik in vielfältiger Form zu unserem alltäglichen Leben: Die Daten auf deiner Krankenkassen-Karte sind verschlüsselt, ebenso die Signale der Pay-TV-Sender und hoffentlich deine Daten beim Einkauf im Internet. Auf vielen Werbeflächen findest du die Schwarz-Weiß-Muster von QR-Codes. In diesen Mustern werden häufig Internet-Adressen von Firmen verschlüsselt. Man kann so aber auch beliebige Texte darstellen.

Die heutigen Verschlüsselungsmethoden nutzen dabei häufig eigentlich einfache Mathematik: Es ist sehr einfach zwei große natürliche Zahlen zu multiplizieren, denn dafür gibt es ein einfaches Verfahren, das du schon aus der Grundschule kennst. Dagegen ist es schwer, eine sehr große natürliche Zahl wieder in ihre Ausgangsfaktoren zu zerlegen. Dies gelingt aber, wenn man den Schlüssel – hier eine der Ausgangszahlen – kennt.

Übrigens: Der QR-Code oben bedeutet: Wir wünschen euch viel Spaß beim Codeknacken.

Wichtige Begriffe - Puzzle

Schneide die einzelnen Teile entlang der feinen Linien aus.



Wichtige Begriffe
- Lösung des Puzzles -

Zu einer Geheimschrift gehören mindestens zwei Personen, eine, die die Nachricht verschlüsselt (**Sender**), und eine, die sie entschlüsselt (**Empfänger**).
Manchmal taucht jemand auf, der die geheime Botschaft ganz ohne den Schlüssel knacken will. Er wird **Angreifer** oder **Codebrecher** genannt.

Die Kunst vom Ver- und Entschlüsseln geheimer Nachrichten heißt **Kryptographie** oder **Kryptologie**.
Das kommt von den griechischen Wörtern „kryptos" (geheim), „logos" (das Wort, der Sinn) und „graphein" (schreiben).

Vor der Verschlüsselung nennt man die Botschaft **Klartext**, nach der Verschlüsselung sagt man dazu **Geheimtext**.

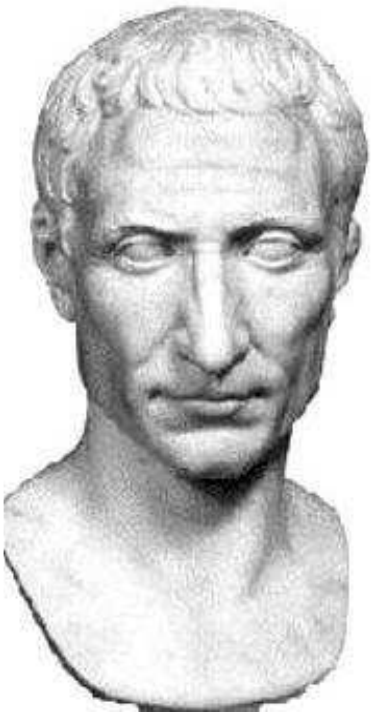
Statt **verschlüsseln** sagt man auch **chiffrieren**, statt **entschlüsseln** auch **dechiffrieren**.

Prinzip von Kerckhoffs:

Die **Sicherheit einer Geheimschrift** darf nicht von der Geheimhaltung der Verschlüsselungsmethode abhängen, denn sie ist meistens bekannt.
Der sogenannte **„Schlüssel" ist das Geheimnis**, das nur der Sender und der Empfänger der Nachricht kennen dürfen. (Bei der Caesar-Verschlüsselung ist dies zum Beispiel die Einstellung der Scheiben.)

Üblicherweise schreibt man den **Klartext** mit **kleinen Buchstaben**, den **Geheimtext** mit **großen Buchstaben**!

Geheimschrift von Julius Caesar



Er kam, sah und ... verschlüsselte.

Julius Caesar lebte von 100 bis 44 v. Chr. und wurde als römischer Feldherr und Staatsmann weltberühmt. Das Wort „Kaiser" ist von seinem Namen abgeleitet. Weniger bekannt dagegen ist die Tatsache, dass er sich als einer der ersten intensiv mit Geheimschriften beschäftigt hat.

In seinem Buch über den gallischen Krieg beschreibt Caesar, wie er bei wichtigen Botschaften die Buchstaben aus dem römischen Alphabet durch griechische ersetzte, um so die Mitteilungen für seine Gegner unlesbar zu machen. Caesar benutzte so häufig Geheimschriften, dass Valerius Probus im 1. Jahrhundert n. Chr. ein ganzes Buch darüber schrieb, das aber leider nicht erhalten geblieben ist. Auch der Biograph Sueton berichtet voller Bewunderung, Caesar habe vertrauliche Briefe in einer Geheimschrift an Cicero geschickt. Sehr genau wird hier das Verschlüsselungsverfahren dargestellt, das noch heute den Namen Caesars trägt: „Er veränderte die Ordnung der Buchstaben derart, dass kein einziges Wort mehr ausgemacht werden konnte. Wenn jemand das entziffern und den In-halt erkennen wollte, so musste er den vierten Buchstaben des Alphabets, also D für A einsetzen und so auch mit den anderen verfahren." (Caes. LVI)

Das klingt zwar recht kompliziert, Caesars System ist aber ganz einfach:

Zunächst schreibt man das normale Alphabet auf, das ist das sogenannte Klaralphabet. Anschließend schreibt man darunter noch ein Alphabet, fängt aber diesmal nicht mit dem A, sondern mit dem Buchstaben D an; das ist das Geheimalphabet.

```
Klar:    a b c d e f g h i j k l m n o p q r s t u v w x y z
         | | | | | | | | | | | | | | | | | | | | | | | | | |
Geheim: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
```

Hat man nun eine Nachricht (Klartext), die man verschlüsseln will, so ersetzt man einfach jeden Buchstaben des Klartextes durch den darunter stehenden Geheimtextbuchstaben. Aus dem Wort „caesar" wird auf diese Weise: FDHVDU

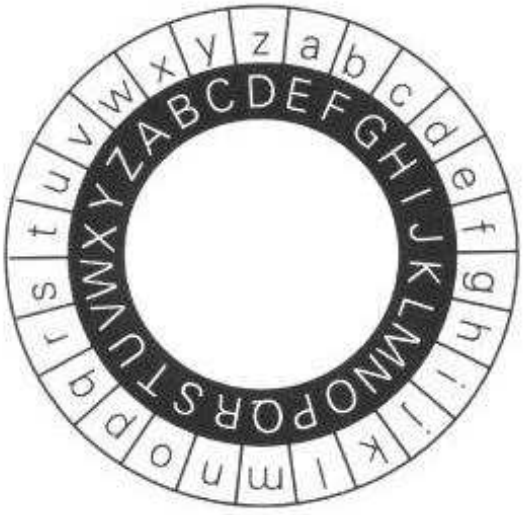
Wenn du einen solchen Geheimtext entschlüsseln willst, gehst du einfach umgekehrt vor. Vielleicht wollte Caesar ja einen Freund warnen und hat ihm geschrieben:

WUDXHQLHGHPEUXWXV

Aufgabe: Schreibe nun selbst eine kleine Nachricht in Caesars Geheimschrift und lasse sie von deinem Nachbarn entschlüsseln.

Caesar-Scheiben

Caesars Geheimschrift bestand darin, dass er das Geheimalphabet gegenüber dem Klaralphabet um drei Buchstaben verschob. Obwohl Sueton nur diese Verschiebung um drei Stellen erwähnt, war Caesar natürlich klar, dass man das Geheimalphabet auch um eine andere Anzahl von Stellen verschieben kann. Auf diese Weise erhält man 25 verschiedene Geheimschriften, denn die 26. Verschiebung liefert dann ja wieder das Klaralphabet.
Um nicht für jede Verschiebung eine neue Tabelle zeichnen zu müssen, kann man auch eine „Chiffriermaschine" wie in der Abbildung rechts benutzen. Diese Maschine besteht aus zwei Scheiben, die so zu drehen sind, dass man die gewünschte Verschiebung einstellen kann; man nennt sie auch Caesar-Scheiben.



Auf der äußeren Scheibe ist das Klaralphabet, auf der inneren Scheibe das Geheimalphabet geschrieben. Dabei verwendet man für den Klartext üblicherweise immer kleine Buchstaben, für den Geheimtext immer große, aber das kennen wir ja schon.
Wenn man die Einstellung der Scheiben so wie auf der Abbildung wählt, wird also der Klartextbuchstabe a durch den Geheimtextbuchstaben E verschlüsselt usw.
Aus dem Namen „adamriese" wird dann der Geheimtext EHEQVMIWI.
Will jemand die Botschaft lesen, so muss er nur wissen, welcher große Buchstabe beim Verschlüsseln unter dem kleinen a stand. Wenn man das nicht weiß, wird die ganze Sache etwas schwieriger, aber es gibt ja zum Glück nur 25 Möglichkeiten.

Chiffrierscheibe der Südstaatenarmee

Bereits 1470 hatte der Italiener Leon Battista Alberti eine solche Maschine erfunden und aus zwei Kupferscheiben angefertigt. Die in der Abbildung gezeigte Version wurde im Amerikanischen Bürgerkrieg von der Südstaatenarmee verwendet.
Der deutsche Erfinder Arthur Scherbius entwickelte ab 1918 eine Verschlüsselungsmaschine, die von den Deutschen im 2. Weltkrieg eingesetzt wurde. Er gab ihr den Namen Enigma. Im Grunde war sie nur eine elektrische Version der Caesar-Scheiben und trotzdem wurde sie zur gefürchtetsten Chiffriermaschine der Geschichte.

Aufgaben:

1. Bastele dir Caesar-Scheiben.
2. Entschlüssele den Geheimtext: MRNBNACNGCRBCWRLQCVNQAPNQNRV
   Der Schlüssel zum Geheimnis ist dabei: a - J
3. Stelle deine Caesar-Scheiben auf den Schlüssel a - Z ein.
   Schreibe nun selbst einen kleinen Satz in Geheimschrift und lasse ihn von deinem Nachbarn entschlüsseln.
4. Ein Grund zum Jubeln: OLBALNPIALZRLPULOHBZHBMNHILU

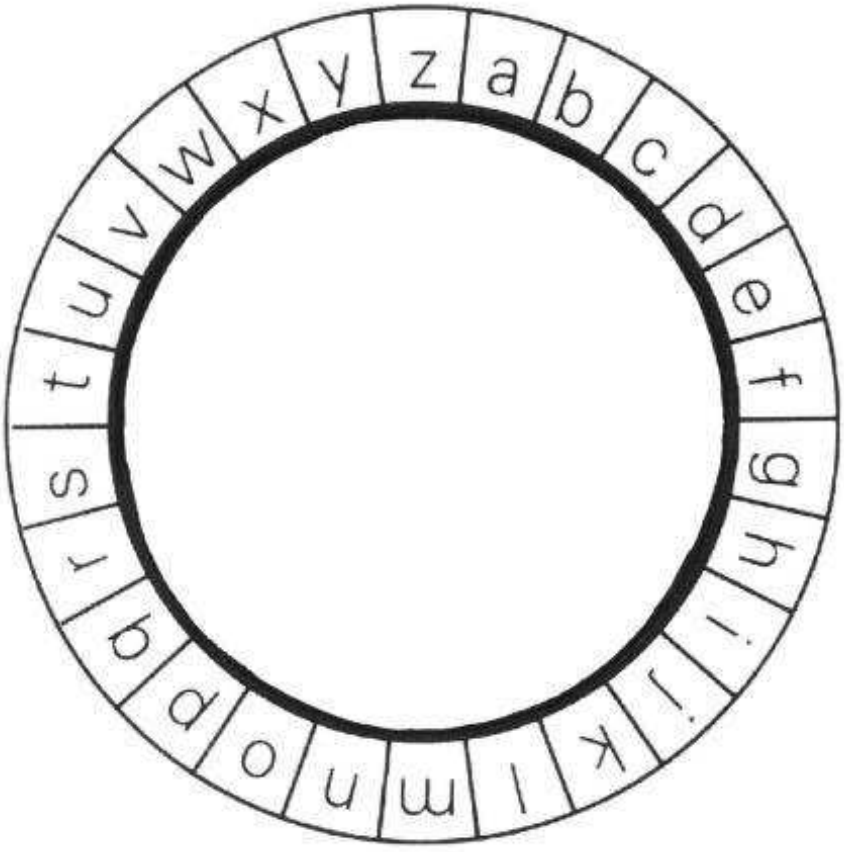
Wir basteln
Caesar-Scheiben

Du brauchst folgende **Materialien**:

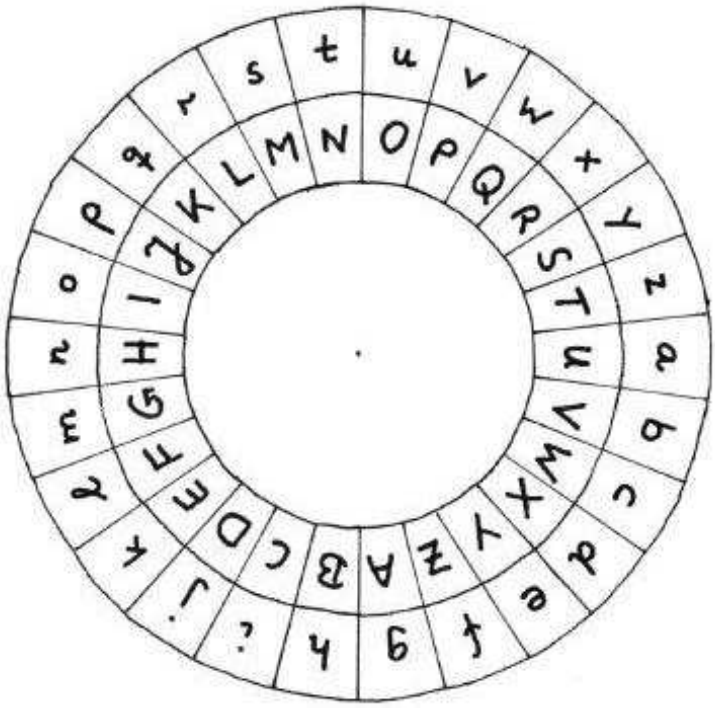
- stabile Pappe (ein DIN-A5-Bogen)
- Schere
- Kleber
- Bleistift und Geodreieck
- eine Briefklammer

Und so geht es:

- Klebe die beiden Scheiben auf die
  schneide sie dann sorgfältig aus.
- Erinnerst du dich noch, wie man den Mittelpunkt eines Kreises nur mit dem Geodreieck bestimmen kann? Gut, dann benutze nun die Rückseite der Scheiben, um beide Mittelpunkte einzuzeichnen.
- Lege jetzt die kleinere auf die größere Scheibe und verbinde beide in der Mitte mit der Briefklammer.
- Wenn du Lust hast, kannst du die Felder bzw. Buchstaben zum Schluss noch mit verschiedenen Farben ausmalen. Schon sind deine Caesar-Scheiben fertig.



Wir basteln Caesar-Scheiben



Du brauchst folgende **Materialien**:

- stabile Pappe (ein DIN-A4-Bogen)
- Zirkel und Geodreieck
- Bleistift und Filzstift
- Schere
- eine Briefklammer

Und so geht es:

- Zeichne mit dem Zirkel drei große Kreise nebeneinander (!) auf die Pappe. Dabei sollte der größte einen Radius von 8 cm, der mittlere einen Durchmesser von 12 cm und der kleinste einen Radius von 4 cm haben. Du kennst doch den Unterschied zwischen Radius und Durchmesser, oder?

- Da das Alphabet 26 Buchstaben hat, musst du die beiden größeren Kreise jetzt in 26 Sektoren unterteilen. Überlege zunächst, wie viel Grad du für jeden Winkel nehmen musst. Dabei wird zwar ein kleines Problem auftauchen, damit wirst du aber bestimmt selbst fertig. Zum Zeichnen der Winkel solltest du das Geodreieck und den Bleistift verwenden. (Vorsicht: Du musst hier ziemlich genau abmessen, sonst kommt es später nicht hin.)

- Nun schneidest du alle drei Kreise sorgfältig aus und ziehst die Bleistiftlinien mit dem Filzstift nach.

- Die beiden größeren Scheiben werden jetzt genau wie auf der Abbildung oben jeweils ganz außen mit dem Alphabet beschriftet (Filzstift). Die größte Scheibe erhält reihum die kleinen Buchstaben, auf die mittlere schreibst du die großen Buchstaben.

- Lege alle drei Scheiben der Größe nach aufeinander und verbinde sie, indem du die Briefklammer durch die Mittelpunkte der Scheiben steckst.

- Wenn du Lust hast, kannst du die Felder zum Schluss noch mit verschiedenen Farben ausmalen. Schon sind deine Caesar-Scheiben fertig.

Das häufige e und das seltene q

In der deutschen Sprache treten die einzelnen Buchstaben des Alphabets in sehr unterschiedlicher Häufigkeit auf, es gibt Buchstaben, die extrem häufig vorkommen und andere, die ganz selten sind. Es handelt sich hier um eine statistische Gesetzmäßigkeit, die man bei längeren Texten recht gut untersuchen kann.

Der mit Abstand häufigste Buchstabe ist mit 17,4% das e. Dies ist natürlich nur ein Durchschnittswert, der nicht bei jedem kleinen Text erreicht wird. So enthält der bekannte Zungenbrecher „In Ulm und um Ulm und um Ulm herum" nur ein einziges e. Allerdings ist es enorm schwierig, einen längeren Text zu schreiben, ohne den Buchstaben e zu verwenden. Im Jahr 1969 schuf der französische Schriftsteller Georges Perec einen Roman von 200 Seiten, in dem der Buchstabe e kein einziges Mal vorkommt. Auch in der deutschen Übersetzung taucht das e nicht auf. Trotzdem kann man den Text ganz gut lesen. Die einleitenden Sätze des Romans finden sich im Kasten rechts.

„Kardinal, Rabbi und Admiral, als Führungstrio null und nichtig und darum völlig abhängig vom Ami-Trust, tat
durch Rundfunk und Plakatanschlag kund, dass Nahrungsnot und damit
Tod aufs Volk zukommt. Zunächst tat man das als Falschinformation ab.
Das ist Propagandagift, sagt man.
Doch bald schon ward spürbar, was man ursprünglich nicht glaubt. Das
Volk griff zu Stock und zu Dolch."

aus: Georges Perec, Anton Voyls Fortgang (Frankfurt a.M. 1991).

Im Gegensatz zum e tauchen die Buchstaben x, y und vor allem q in der deutschen Sprache so gut wie nicht auf.

Aufgabe: Versuche doch selbst einmal, einen Satz ohne e zu schreiben. Kannst du auch einen Satz formulieren, in dem die Buchstaben x,y und q besonders häufig sind?

Das Probieren aller 25 Möglichkeiten bei der Entschlüsselung von Geheimtexten, die mit den Caesar-Scheiben geschrieben wurden, ist ziemlich lästig. Wenn man jetzt aber die unterschiedliche Häufigkeit der Buchstaben berücksichtigt, können wir viel raffinierter vorgehen.
Gehen wir also zunächst davon aus, dass der Buchstabe e der häufigste Buchstabe im Klartext gewesen ist. Dann muss ja der Buchstabe, in den e verschlüsselt wird, der häufigste Buchstabe im Geheimtext sein.
Wenn wir also jetzt umgekehrt den häufigsten Buchstaben im Geheimtext ausfindig machen können, so wird dieser mit ziemlich großer Wahrscheinlichkeit dem e im Klartext entsprechen. Wir müssen dann die Caesar-Scheiben nur noch auf diese Kombination einstellen und schon können wir den Geheimtext entschlüsseln.

Aufgabe:
NBPRKCWDAMANRBXACNWEXWVJCQNVJCRTUNQANAW
BXULQNMRNKRBMANRIJNQUNWTXNWWNW
DWMBXULQNMRNMJBWRLQCTXNWWNW

1. Notiere in einer Strichliste, wie oft die einzelnen Buchstaben im Geheimtext vorkommen.
2. Gib jetzt in einer Tabelle mit den Buchstaben von A bis Z die absoluten Häufigkeiten an. Zeichne dazu ein Balkendiagramm.
3. Überführe die Tabelle in eine Rangliste.
4. Stelle die Caesar-Scheiben so ein, dass der häufigste Buchstabe des Geheimtextes dem Buchstaben e des Klartextes entspricht und entschlüssele den Text.

Das häufige e und das seltene q
- Lösungen -

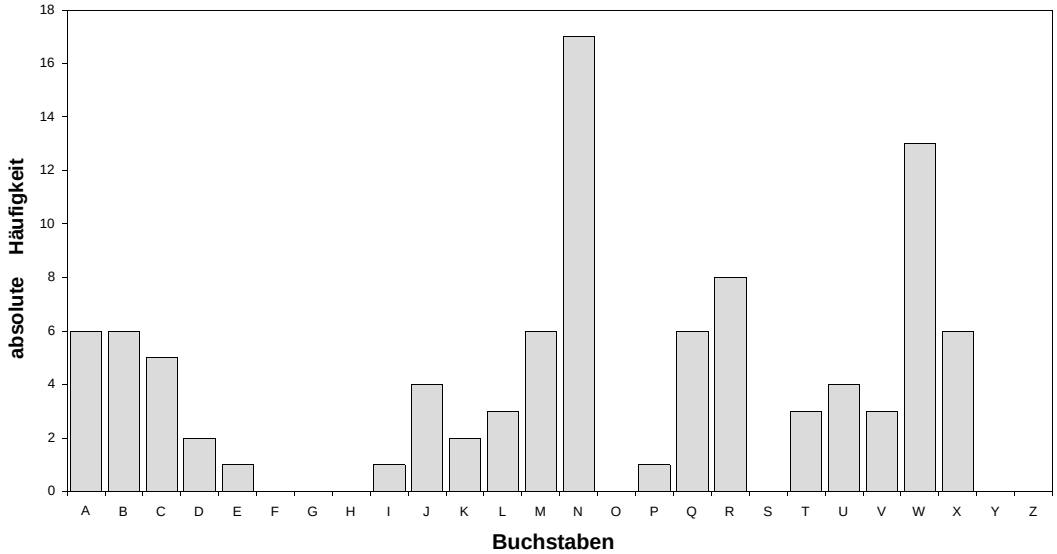
Häufigkeitstabelle

	Strichliste	absolute Häufigkeiten	Klartextbuchstabe
A	𝍸	6	r
B	𝍸	6	s
C	𝍸	5	t
D	||	2	u
E	|	1	v
F			w
G			x
H			y
I	|	1	z
J	||||	4	a
K	||	2	b
L	|||	3	c
M	𝍸	6	d
N	𝍸 𝍸 𝍸 ||	17	e
O			f
P	|	1	g
Q	𝍸	6	h
R	𝍸 |||	8	i
S			j
T	|||	3	k
U	||||	4	l
V	|||	3	m
W	𝍸 𝍸 |||	13	n
X	𝍸	6	o
Y			p
Z			q

Rangliste

Rang		absolute Häufigkeiten	Klartextbuchstabe
1	N	17	e
2	W	13	n
3	R	8	i
4	A	6	r
4	B	6	s
4	M	6	d
4	Q	6	h
4	X	6	o
5	C	5	t
6	J	4	a
6	U	4	l
7	L	3	c
7	T	3	k
7	V	3	m
8	D	2	u
8	K	2	b
9	E	1	v
9	I	1	z
9	P	1	g
10	F		w
10	G		x
10	H		y
10	O		f
10	S		j
10	Y		p
10	Z		q

Balkendiagramm



nur drei sorten von mathematiklehrern
die bis drei zaehlen koennen
und solche die das nicht koennen

Wir zählen Buchstaben

Wie wir schon gesehen haben, tauchen die verschiedenen Buchstaben in einem „normalen deutschen Text" unterschiedlich oft auf. Wir werden das nun genauer untersuchen, denn damit lassen sich sehr viele Geheimschriften knacken. Man kann sogar sagen, dass eine Häufigkeitsanalyse der Buchstaben das wichtigste Werkzeug bei der Entschlüsselung von Geheimtexten ist.

Aufgabe:
Wähle eine Zahl zwischen 5 und 150 und schlage danach die entsprechende Seite in deinem Deutschbuch auf.
Fange mit deiner Untersuchung nun oben an und notiere in einer Strichliste, wie oft die einzelnen Buchstaben vorkommen. Dabei sollst du Leer- und Satzzeichen nicht berücksichtigen, jedes ß durch ss ersetzen und die Umlaute ä, ö und ü wie ae, oe und ue behandeln. Höre auf, wenn du genau 400 Buchstaben gezählt hast.
Berechne dann bei jedem Buchstaben zur absoluten auch die relative Häufigkeit.

	MEINE ERGEBNISSE		
Buchstabe	**Strichliste**	**absolute Häufigkeit**	**relative Häufigkeit**
a			
b			
c			
d			
e			
f			
g			
h			
i			
j			
k			
l			
m			
n			
o			
p			
q			
r			
s			
t			
u			
v			
w			
x			
y			
z			

	ERGEBNISSE MEINER GRUPPE		ERGEBNISSE MEINER KLASSE	
	absolute	relative	absolute	relative
Buchstabe	Häufigkeit	Häufigkeit	Häufigkeit	Häufigkeit
a				
b				
c				
d				
e				
f				
g				
h				
i				
j				
k				
l				
m				
n				
o				
p				
q				
r				
s				
t				
u				
v				
w				
x				
y				
z				

Aufgabe:

Arbeite nun mit den relativen Häufigkeiten, die von der gesamten Klasse ermittelt wurden (letzte Spalte).

1. Fertige dazu ein passendes Balkendiagramm an.
2. Vergleiche dieses Balkendiagramm mit dem, welches du bei der Entschlüsselung des letzten Geheimtextes angefertigt hast. Was stellst du fest?
3. Was soll das?

> Im Deutschen sind besonders auffällig die e-Spitze und der n-Gipfel,
> die f-g-h-i-Flanke mit anschließender j-k-Senke,
> die o-p-q-Senke mit anschließendem r-s-t-u-Kamm.
> (aus: Friedrich L. Bauer, Entschlüsselte Geheimnisse)

4. Erstelle für die relativen Häufigkeiten eine Rangliste.
5. Überlege dir eine sinnvolle Klasseneinteilung und stelle diese in einem Kreisdiagramm dar.

Häufigkeitsverteilung der Buchstaben des deutschen Alphabets

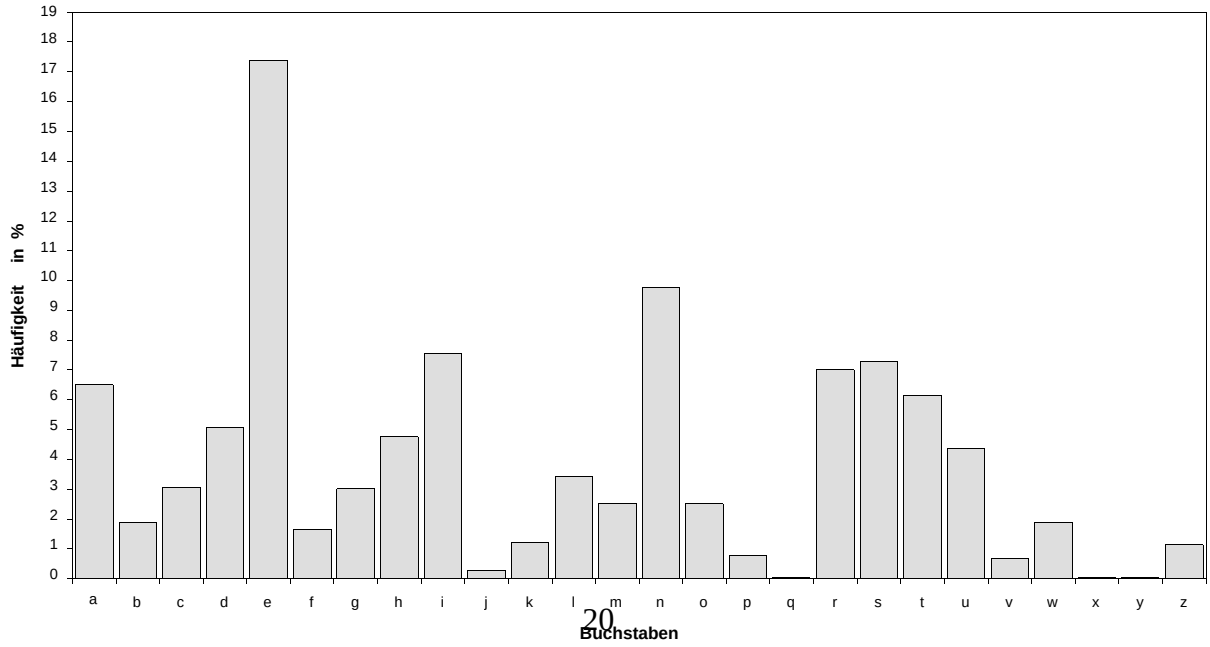
nach dem Alphabet

Buchstabe	Häufigkeit (in %)
a	6,51
b	1,89
c	3,06
d	5,08
e	17,40
f	1,66
g	3,01
h	4,76
i	7,55
j	0,27
k	1,21
l	3,44
m	2,53
n	9,78
o	2,51
p	0,79
q	0,02
r	7,00
s	7,27
t	6,15
u	4,35
v	0,67
w	1,89
x	0,03
y	0,04
z	1,13

nach der Häufigkeit

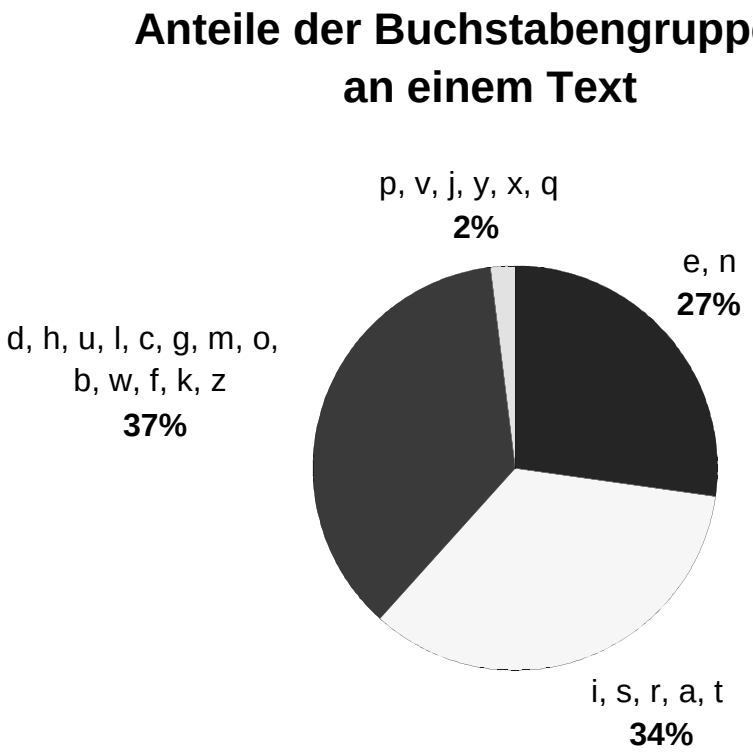
Buchstabe	Häufigkeit (in %)
e	17,40
n	9,78
i	7,55
s	7,27
r	7,00
a	6,51
t	6,15
d	5,08
h	4,76
u	4,35
l	3,44
c	3,06
g	3,01
m	2,53
o	2,51
b	1,89
w	1,89
f	1,66
k	1,21
z	1,13
p	0,79
v	0,67
j	0,27
y	0,04
x	0,03
q	0,02

Häufigkeitsverteilung der Buchstaben in der deutschen Sprache



nach Buchstabengruppen

Gruppe	Anteil der Buchstaben dieser Gruppe an einem Text
e, n	27,18%
i, s, r, a, t	34,48%
d, h, u, l, c, g, m, o, b, w, f, k, z	36,52%
p, v, j, y, x, q	1,82%



Die häufigsten Bigramme in der deutschen Sprache:

Buchstabenpaar	en	er	ch	te	de	nd	ei	ie	in	es
Häufigkeit (in%)	3,88	3,75	2,75	2,26	2,00	1,99	1,88	1,79	1,67	1,52

nach: A. Beutelspacher, Kryptologie (Wiesbaden 1996).

Caesar mit Schlüsselwort

Hat man eine wirklich wichtige Nachricht, so reichen 25 verschiedene Geheimschriften einfach nicht aus; zu groß ist die Gefahr, dass der Geheimtext geknackt wird.

Statt das Alphabet nur zu verschieben, kann man als Geheimalphabet auch beliebige Umstellungen des Klaralphabets zulassen. Auf diese Weise lässt sich eine sehr viel größere Zahl unterschiedlicher Geheimschriften erzeugen.

Was hältst du zum Beispiel von folgender Zuordnung?

Klar:	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|
Geheim:	**M**	**R**	**Z**	**E**	**N**	**S**	**C**	**V**	**X**	**D**	**K**	**U**	**A**	**O**	**L**	**F**	**Q**	**W**	**B**	**T**	**Y**	**I**	**G**	**P**	**H**	**J**

Aufgabe: Wie kann man die Anzahl aller so herstellbaren Geheimschriften berechnen?

Das Schöne an dieser Verschlüsselung ist, dass sie leicht anzuwenden ist und eine sehr große Sicherheit bietet. Eine Geheimschrift sollte möglichst einfach sein, damit es nicht so leicht zu Missverständnissen kommt. Der Absender braucht nur die Rei- henfolge der 26 Buchstaben festzulegen, der Empfänger kann die Nachricht mit Hilfe der Tabelle leicht entschlüsseln.

Aufgabe: EMBGMWGXWKUXZVOXZVTBZVGNW

Das größte Problem bei diesem Verfahren ist, dass die Tabelle verloren gehen könnte. Dann ist es schwierig, die Nachricht trotzdem zu knacken.
Aus diesem Grund ordnet man die Buchstaben des Geheimalphabets besser nicht rein zufällig, sondern mit Hilfe eines Schlüsselworts, an das man sich später noch gut erinnern kann.

Auch dazu ein **Beispiel**:

- Als Schlüsselwort wählen wir etwa: JULIUS CAESAR
- Dann lässt man zuerst die Wortzwischenräume weg: JULIUSCAESAR
- Kommt ein Buchstabe mehrmals im Schlüsselwort vor, so bleibt er nur beim ersten Mal stehen: JULISCAER
  Dieses Wort wird jetzt als Beginn des Geheimalphabets verwendet.
- Das Geheimalphabet füllt man jetzt mit einem verschobenen Alphabet auf. Man beginnt dort, wo das Schlüsselwort endet. Die Buchstaben, die schon im Schlüsselwort vorkommen, werden dabei einfach weggelassen.
- Die Verschlüsselungstabelle sieht also so aus:

Klar:	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|
Geheim:	**J**	**U**	**L**	**I**	**S**	**C**	**A**	**E**	**R**	**T**	**V**	**W**	**X**	**Y**	**Z**	**B**	**D**	**F**	**G**	**H**	**K**	**M**	**N**	**O**	**P**	**Q**

Aufgabe: Probiere es nun selbst einmal.
Erstelle für das Schlüsselwort BLEISTIFT die Verschlüsselungstabelle und schreibe in dieser Geheimschrift: mathe macht spass .

Auch wenn man mit einem Schlüsselwort arbeitet, ist eine große Sicherheit immer noch gewährleistet. Durch Probieren lässt sich eine Nachricht wegen der großen Anzahl an Möglichkeiten kaum entschlüsseln. Das glaubst du nicht? Dann versuche es doch einmal mit dem folgenden Text. Freundlicherweise sind die Wörter diesmal durch Leerzeichen voneinander getrennt.

```
UMVRTA HNVFAZ JAZBDMAVFNLAV BNRT LAZVA UND IABWVFAZAV
LATANUQANRTAV
ANVA BWSRTA LATANUBXZMRTA NBD MIAZ VNRTD BATZ BNRTAZ
FMTAZ JAZKAVFADA RMABMZ MGRT VGZ FNA VWZUMSAV
IGRTBDMIAV
```

Aber wir waren ja auch schon einen Schritt weiter: die Häufigkeitsanalyse der Buchstaben! Wenn wir die Buchstaben in unserem Geheimtext zählen, so erhält man folgende Tabellen:

Häufigkeitstabelle

	absolute Häufigkeiten
A	32
B	10
C	0
D	6
E	0
F	6
G	3
H	1
I	4
J	2
K	1
L	4
M	10
N	12
O	0
P	0
Q	1
R	10
S	2
T	13
U	5
V	15
W	3
X	1
Y	0
Z	13

Rangliste

Rang		absolute Häufigkeiten
1	A	32
2	V	15
3	T	13
3	Z	13
4	N	12
5	B	10
5	M	10
5	R	10
6	D	6
6	F	6
7	U	5
8	I	4
8	L	4
9	G	3
9	W	3
10	J	2
10	S	2
11	H	1
11	K	1
11	Q	1
11	X	1
12	C	0
12	E	0
12	O	0
12	P	0
12	Y	0

Wie erwartet kommen die Buchstaben unterschiedlich oft vor. Mit großem Abstand ist das A der häufigste Buch- stabe im Geheimtext, wir können daher fast sicher sein, dass es sich hier um den Klartextbuchstaben e handelt.

Jetzt wird die Sache etwas schwieriger, da sich die Häufigkeiten der nächsten Buch- staben in der Rangliste kaum voneinander unterscheiden. Aber weil alles sowieso auf Statistik beruht, darf man sich eh nicht hundertprozentig sicher sein. Stattdessen sollte man stets nach Bestätigungen für seine Vermutungen Ausschau halten. Da uns zu diesem Zeitpunkt nichts anderes übrig bleibt, gehen wir zunächst davon aus, dass der zweite Buch- stabe in der Rangliste (also das V) auch dem zweithäufigsten Buchstaben in der deutschen Sprache (also dem n) entspricht.

Setzt man die beiden Buchstaben e und n in den Geheimtext ein, so erhält man:

```
UMnRTe HNnFeZ JeZBDMenFNLen BNRT LeZne UND IeBWnFeZen
LeTeNUQeNRTen
eNne BWSRTe LeTeNUBXZMRTe NBD MIeZ nNRTD BeTZ BNRTeZ
FMTeZ JeZKenFeDe RMeBMZ MGRT nGZ FNe nWZUMSen
IGRTBDMIen
```

Jetzt geht man den Text Wort für Wort durch und versucht etwas Auffälliges zu finden. In der dritten Zeile steht die Buchstabenkombination `eNne` . Wenn die beiden ersten Ersetzungen richtig waren, könnte es sich hier um das Wort `eine` handeln, der Buchstabe N müsste dann durch ein i ersetzt werden. Da das N im Geheimtext recht häufig ist, könnte es stimmen. Das probieren wir gleich aus:

```
UMnRTe HinFeZ JeZBDMenFiLen BiRT LeZne UiD IeBWnFeZen
LeTeiUQeiRTen
eine BWSRTe LeTeiUBXZMRTe iBD MIeZ niRTD BeTZ BiRTeZ
FMTeZ JeZKenFeDe RMeBMZ MGRT nGZ Fie nWZUMSen
IGRTBDMIen
```

Haben wir uns doch vertan? Man kann ja fast nichts mehr erkennen, so unübersichtlich wird das hier. Aber das haben wir gleich.

```
**n**e *in*e* *e****en*i*en *i** *e*ne *i* *e**n*e*en
*e*ei**ei**en
eine *****e *e*ei*******e i** **e* ni*** *e** *i**e*
***e* *e**en*e*e **e*** **** n** *ie n*****en
********en
```

In der dritten Zeile findet man nun `ni***` . Ein Blick in den Duden zeigt uns, dass es eigentlich nur ein sinnvolles Wort mit fünf Buchstaben gibt, das mit `ni` beginnt; es ist das Wort `nicht`.
Dazu passt auch die Tatsache, dass die Buchstabenkombination `RT` mehrmals im Geheimtext vorkommt, das `ch` ist eine der häufigsten Buchstabenkombinationen in unserer Sprache.
Wir setzen die entsprechenden Buchstaben ein und erhalten:

```
UMnche HinFeZ JeZBtMenFiLen Bich LeZne Uit IeBWnFeZen
LeheiUQeichen
eine BWSche LeheiUBXZMche iBt MIeZ nicht BehZ BicheZ
FMheZ JeZKenFete cMeBMZ MGch nGZ Fie nWZUMSen
IGchBtMIen
```

Jetzt geht es immer schneller. Das erste Wort lässt sich leicht entschlüsseln.

```
manche HinFeZ JeZBtaenFiLen Bich LeZne mit IeBWnFeZen
LeheimQeichen
eine BWSche LeheimBXZache iBt aIeZ nicht BehZ BicheZ
FaheZ JeZKenFete caeBaZ aGch nGZ Fie nWZmaSen
IGchBtaIen
```

Der Rest ergibt sich fast von selbst und wir erhalten als Klartext:

```
manche kinder verstaendigen sich gerne mit besonderen
geheimzeichen
eine solche geheimsprache ist aber nicht sehr sicher
daher verwendete caesar auch nur die normalen
buchstaben
```

Bei der Verschlüsselung verwendete man also folgende Tabelle:

Klar:	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|
Geheim:	**M**	**I**	**R**	**F**	**A**	**E**	**L**	**T**	**N**	**C**	**H**	**S**	**U**	**V**	**W**	**X**	**Y**	**Z**	**B**	**D**	**G**	**J**	**K**	**O**	**P**	**Q**

Das Schlüsselwort ist: MIR FAELLT NICHTS EIN

Mit der Häufigkeitsanalyse und einer guten Portion Erfahrung lassen sich also auch solche Texte knacken, die nach dem Caesar-Verfahren mit Schlüsselwort erstellt wurden. Je länger diese Geheimtexte sind, umso leichter kommt man dem Geheim- nis auf die Spur. Wenn sie dagegen weniger als 100 Buchstaben haben, ist die Ent- schlüsselung normalerweise fast unmöglich.

Aufgabe: Der Text auf dem nächsten Blatt wurde nach dem gleichen Verfahren verschlüsselt. Vermutlich wird er dir recht bald sehr bekannt vorkommen. Oder bist du keine Lese-Ratte?
Erstelle zunächst eine Häufigkeitstabelle und eine Rangliste, dann kann es gleich losgehen.
Vielleicht setzt du für diese Aufgabe auch einen Computer ein, das ist zwar nicht erforderlich, aber etwas komfortabler.

YQBUFOMMXJOZ

OD NFY OTZRFI OTZ RFOAXJOZ, AFD NOWOZ DOTZOY YQBOZ CFDOXFM FID YQBUFOMMXJOZ AOLTZTOYB NEYAO. ATO REBBOY LQYREITOYBO ATO FELWFCO: "WOJO KEY WYQDDREBBOY. WOJO ZTXJB TR AYOTOXU QAOY TR YOXJBOZ NTZUOI, DQZAOYZ DEXJO ATO UEOYKODBO GOYCTZAEZW AOD NOWOD. FAATOYO ATO CIEROZ FR NOWYFZA KE OTZOR NEZAOYDXJQOZOZ DBYFEDD EZA UEOYKO TJZ DQNOTB NTO RQOWITXJ."

YQBUFOMMXJOZ DERRTOYBO OTZOZ UEXJOZ, OTZO NEYDB EZA OTZO LIFDXJO NOTZ TZ OTZOR UQYC FEL. FEL AOR NOW KEY WYQDDREBBOY COWOWZOBO AOR RFOAXJOZ TZ AOY ROJYOYO JF WYQDDOZ LIFOXJO AOD NFIAOD, AEYXJ AOZ OD WTZW, KELFOIITW OTZ NQIL, QCNQJI ATO NFJYDXJOTZITXJUOTB AFLEOY ZFJOKE ZEII NFY. AFD BTOY ERUYOTDBO YQBUFOMMXJOZ TR DBOBD WIOTXJOZ FCDBFZA. AFCOT LYFWBO AOY NQIL DTO ZFXJ TJYOR ZTOI EZA OYREZBOYBO DTO ZQXJ NOTBOYO CIEROZ KE MLIEOXUOZ, ER AOZ DBYFEDD KE OYNOTBOYZ.

OY DOICDB FCOY OZBLOYZBO DTXJ.

FID YQBUFOMMXJOZ DMFOBOY ATO DBOTWEZW AOD WOYFAOZ FZDBTOWD KER JFED AOY WYQDDREBBOY WOZQRROZ JFBBO, COROYUBO DTO OTZOZ CODOZ ZOCOZ AOY JFEDBüY, AODDOZ UOJYNOYB DOJY UIOTZ NFY, NOTI OY UFER ZQXJ CQYDBOZ JFBBO. TR JFED BYFL DTO ATO WYQDDREBBOY TR COBB FZ. DTO LYFWBO: "WYQDDREBBOY, NFYER JFDB AE DQ WYQDDO FEWOZ?" "TXJ JFCO LYEOJOY TRROY GOYDEXJB COT ROTZOR ZFXJCFYZ FCKEDXJYOTCOZ!" "WYQDDREBBOY, NFYER JFDB AE DQ WYQDDO QJYOZ?" "TXJ JFCO ROTZ JFZAH TRROY FEL IFEBIQD WODBOIIB EZA NTII UOTZOZ FZYEL GOYMFDDOZ!" "WYQDDREBBOY, NFYER JFDB AE DQ OTZ WYQDDOD RFEI?" "TXJ JFCO TRROY GOYDEXJB, ROTZOZ CEYWOY WFZK TZ AOZ REZA KE DXJTOCOZ!"

AFYFEL LYFDD AOY NQIL AFD YQBUFOMMXJOZ.

OTZ PFOWOY UFR, DFJ, AFDD ATO FCDQIEBO JFOELTWUOTB GQZ WYQDDREOBBOYZ TR JFED ZEII NFY. AFZZ ZFJR OY DOTZ RODDOY EZA DECBYFJTOYBO ATO QRF EZA YQBUFOMMXJOZ GQR NQIL. ZER NQIL NEYAO OTZO WYQDDO ROZWO GQZ DBOTZOZ JTZKEWOLüWB. OY LTOI TZ OTZOZ KHITZAOYLQOYRTWOZ CYEZZOZ.

Caesar mit Schlüsselwort - Lösung

rotkaeppchen

es war einmal ein maedchen, das wegen seiner roten basecap als rotkaeppchen definiert wurde. die mutter formulierte die aufgabe: "gehe zur grossmutter. gehe nicht im dreieck oder im rechten winkel, sondern suche die kuerzeste verbindung des weges. addiere die blumen am wegrand zu einem wunderschoenen strauss und kuerze ihn soweit wie moeglich."

rotkaeppchen summierte einen kuchen, eine wurst und eine flasche wein in einem korb auf. auf dem weg zur grossmutter begegnete dem maedchen in der mehrere ha grossen flaeche des waldes, durch den es ging, zufällig ein wolf, obwohl die wahrscheinlichkeit dafuer nahezu null war. das tier umkreiste rotkaeppchen im stets gleichen abstand. dabei fragte der wolf sie nach ihrem Ziel und ermunterte sie noch weitere blumen zu pfluecken, um den strauss zu erweitern.

er selbst aber entfernte sich.

als rotkaeppchen spaeter die steigung des geraden anstiegs zum haus der grossmutter genommen hatte, bemerkte sie einen besen neben der haustür, dessen kehrwert sehr klein war, weil er kaum noch borsten hatte. im haus traf sie die grossmutter im bett an. sie fragte: "grossmutter, warum hast du so grosse augen?" "ich habe frueher immer versucht bei meinem nachbarn abzuschreiben!" "grossmutter, warum hast du so grosse ohren?" "ich habe mein handy immer auf lautlos gestellt und will keinen anruf verpassen!" "grossmutter, warum hast du so ein grosses maul?" "ich habe immer versucht, meinen burger ganz in den mund zu schieben!"

darauf frass der wolf das rotkaeppchen.

ein jaeger kam, sah, dass die absolute haeufigkeit von grossmuettern im haus null war. dann nahm er sein messer und subtrahierte die oma und rotkaeppchen vom wolf. Zum wolf wurde eine grosse menge von steinen hinzugefügt. er fiel in einen zylinderfoermigen brunnen.

Vigenère-Verschlüsselung

Jahrhunderte lang hatte die Verschlüsselung mit nur einem Geheimalphabet ausreichend Sicherheit geboten. Erst als man die Häufigkeitsanalyse der Buchstaben entwickelt hatte, musste man wieder damit rechnen, dass geheime Nachrichten von einem Übeltäter geknackt werden konnten.
Die Kryptographen waren aber bereit, aus den Fehlern der Vergangenheit zu lernen. Eine verbesserte Geheimschrift sollte so viele Möglichkeiten zur Verschlüsselung bieten, dass man einen Geheimtext allein durch Ausprobieren nicht entschlüsseln kann. Zudem musste man nun für eine gleichmäßigere Verteilung der einzelnen Buchstaben im Geheimtext sorgen, um einen Angriff über die Häufigkeitsanalyse zu verhindern.
Der italienische Mathematiker Alberti schlug deshalb schon um das Jahr 1470 vor, die Einstellung der Caesar-Scheiben beim Verschlüsseln zu verändern und so ständig zwischen zwei oder mehreren Geheimalphabeten hin und her zu springen. Diese Idee wurde von einigen Gelehrten aufgegriffen und weiter entwickelt, der wichtigste unter ihnen war der französische Diplomat Blaise de Vigenère.

Im Jahr 1586 veröffentlichte Vigenère sein Verfahren, bei dem insgesamt 26 verschiedene Geheimalphabete im Wechsel benutzt werden, um eine Botschaft zu verschlüsseln.

Blaise de Vigenère (1523 - 1596)

Man benötigt dabei zunächst ein sogenanntes Vigenère-Quadrat wie auf der nächsten Seite. Hier stehen unter einem Klaralphabet alle 26 Geheimalphabete, jedes davon gegenüber dem vorhergehenden um einen Buchstaben verschoben. Im Grunde handelt es sich also um eine Aufstellung aller Caesar-Verschiebungen.

Außerdem braucht man unbedingt ein zwischen dem Sender und dem Empfänger vereinbartes Schlüsselwort. Die einzelnen Buchstaben des Schlüsselworts entscheiden nun darüber, nach welchem Geheimalphabet ein bestimmter Buchstabe des Klartextes verschlüsselt wird.

Dazu ein **Beispiel:**

- Als Schlüsselwort wählen wir: HALLO
- Der Klartext ist das Wort: kryptographie
- Jetzt schreiben wir das Schlüsselwort so oft wie nötig zeichenweise über den Klartext.

```
Schlüsselwort: H A L L O H A L L O H A L
Klartext:      k r y p t o g r a p h i e
Geheimtext:    ? ? ? ? ? ? ? ? ? ? ? ?
```

- Die Buchstaben des Geheimtextes erhalten wir nun auf folgende Weise:
  Über dem ersten Buchstaben k des Klartextes steht ein H, also wird das k nach dem Geheimalphabet verschlüsselt, das mit einem H beginnt.

In der H-Zeile und der k-Spalte des Vigenère-Quadrats steht der Buchstabe R.
Der erste Buchstabe des Geheimtextes ist gefunden.

- Der zweite Buchstabe des Klartextes ist ein r, darüber steht ein A. Im Vigenère-Quadrat steht in der A-Zeile und der r-Spalte rein zufällig wieder ein R.
- In gleicher Weise werden nun alle Buchstaben des Klartextes verschlüsselt.
  Am Ende erhält man:

```
Schlüsselwort: H A L L O H A L L O H A L
Klartext:      k r y p t o g r a p h i e
Geheimtext:    R R J A H V G C L D O I P
```

Bei diesem Beispiel wird also mit vier verschiedenen Geheimalphabeten gearbeitet.
Der große Vorteil dieses Verfahrens ist leicht zu erkennen: das erste r im Klartext „kryptographie" wird zu einem R verschlüsselt, das zweite r dagegen zu einem C. Umgekehrt steht R einmal für k, im zweiten Fall aber für r.
Das muss alle Geheimschriftenknacker doch wahnsinnig machen, oder?

Hier nun das **Vigenère-Quadrat:**

```
a b c d e f g h i j k l m n o p q r s t u v w x y z

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
V W X Y Z A B C D E F G H I J K L M N O P Q R S T U
W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
Z A B C D E F G H I J K L M N O P Q R S T U V W X Y
```

Obwohl die Verschlüsselungsmethode von Vigenère einfach genial war und eine sehr große Sicherheit bot, wurde sie lange Zeit überhaupt nicht beachtet. Nach sei- nem Tod geriet das Verfahren völlig in Vergessenheit und tauchte erst im 19. Jahr- hundert wieder auf. Fast 300 Jahre lang konnte diese Geheimschrift von niemandem geknackt werden.

Aufgaben:

1. Verschlüssele deinen Vornamen nach dem Vigenère-Verfahren mit dem Schlüsselwort AUTOBAHN.
2. Da sämtliche Geheimalphabete des Vigenère-Quadrats ja auch auf den Caesar- Scheiben eingestellt werden können, kann man die neue Verschlüsselungsmethode auch damit durchführen. Man muss nur daran denken, die Scheiben bei jedem einzelnen Buchstaben auf das neue Geheimalphabet einzustellen.
   Probiere es mit dem Klartext allesklar und dem Schlüsselwort SUPER .

3. Auch der nachfolgende Text wurde mit einer Vigenère-Verschlüsselung erstellt.
   Da wir das Schlüsselwort nicht kennen, wird uns der Inhalt des Textes unbekannt bleiben.
   Erstelle für die Buchstaben des Geheimtextes trotzdem eine Häufigkeitstabelle und stelle die relativen Häufigkeiten in einem Balkendiagramm dar.

```
PRYPRYTLULYMJLYUEGDEFKVUUHFLFNLICUWNL
MHHVGLVBVPTMEYSPYYQCAWYPRYYJLHYOUHMLM
HLRTDICRMHKILUHCLOCUHYYLCLWMLRBHIHZIF
BRXNVYAIFKMYMVUBEVLVQHVCOVYZXCLJGBXNL
VXHHCLVCJLNPKYTYNAILKILIICKIHZGBVRPVV
YPRJHELQEBYIHNIMASLIIHDEL
KMYMEGPPCLPYIXYNPOLGESMWOYHKDOMVCLHYU
QCAICUEHKILDIHUROYRCJLNKMYISYZITBRALH
YYWNPIZTYNAILNIQLWYUAULVYZMYTEWOXYKIG
TEHUYHKHYUOCUHYYRXHWFLFYUDOYLILPFLFYZ
SHKILZEFZMGSEHKICUIAYSMZIBBRALVMUSNHY
MIVUJLOUHXHWNHIASMWOIVYSNKEMKMYMEGPPC
LFLHYWOXYPQGLVNLYLLVQBVXL
```

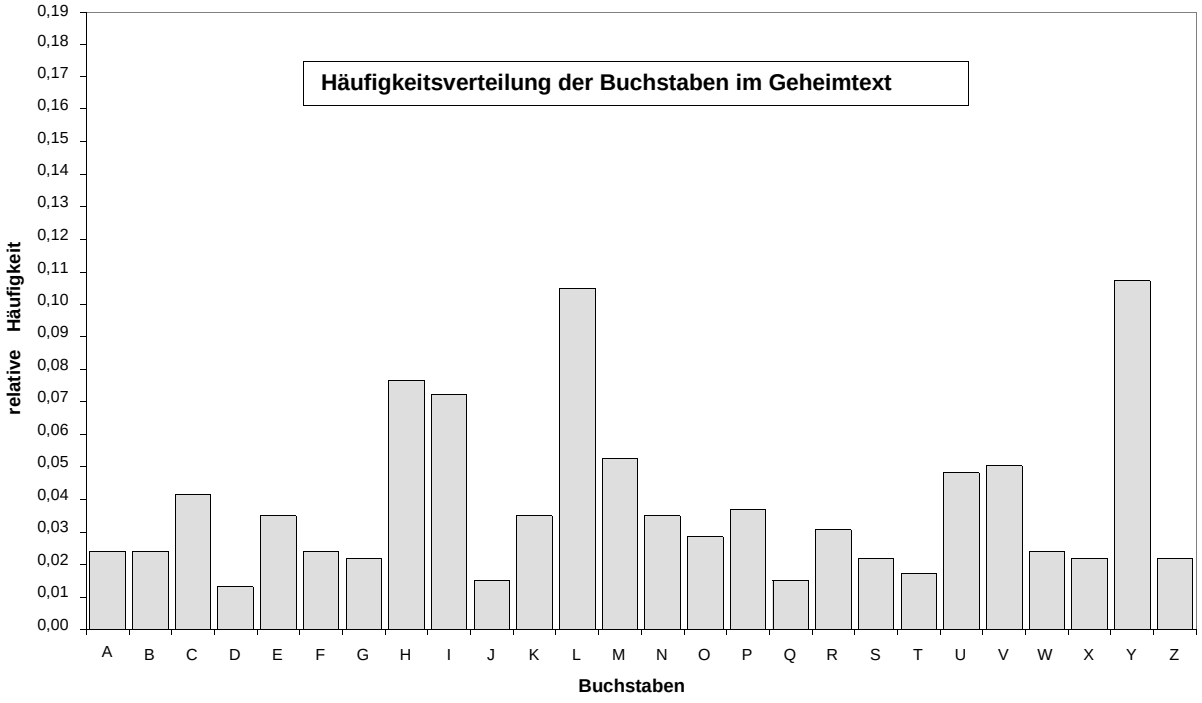
4. Begründe, dass man an diesem Balkendiagramm den großen Vorteil der Vigenère-Methode gut erkennen kann. Was genau ist mit der Häufigkeitsverteilung der Buchstaben geschehen?
5. Aus der Nachbarklasse, mit der ihr das Schlüsselwort KATZE vereinbart habt, erreicht euch folgende Botschaft: CEGCIDBBSXOHBKJO

Könnt ihr damit etwas anfangen?

Vigenère - Lösung

Die Buchstaben in diesem Geheimtext sind sehr viel gleichmäßiger verteilt als bei jedem „normalen Text", da eine poly- alphabetische Verschlüsselung stets die charakteristischen Häufigkeiten der Buchstaben einer Sprache verwischt.
Das wird vor allem deutlich, wenn man das Balkendiagramm unten mit dem zur „Häufigkeitsverteilung der Buchstaben des deutschen Alphabets" vergleicht. La- gen dort die Häufigkeiten des Klartextes zwischen 0,02% und 17,4%, so liegen die des Geheimtextes hier zwischen 1,31% und 10,72%.
Eine Zuordnung zu bestimmten Klartextbuchstaben ist so kaum mehr möglich.
In der Praxis wird man allerdings sehr viel längere Schlüsselwörter verwenden, um ein noch einheitlicheres Bild zu er- halten. Je länger das Schlüsselwort ist, umso ausgeglichener werden die Häufigkeiten.

Buchstabe	absolute Häufigkeit	relative Häufigkeit
A	11	2,41%
B	11	2,41%
C	19	4,16%
D	6	1,31%
E	16	3,50%
F	11	2,41%
G	10	2,19%
H	35	7,66%
I	33	7,22%
J	7	1,53%
K	16	3,50%
L	48	10,50%
M	24	5,25%
N	16	3,50%
O	13	2,84%
P	17	3,72%
Q	7	1,53%
R	14	3,06%
S	10	2,19%
T	8	1,75%
U	22	4,81%
V	23	5,03%
W	11	2,41%
X	10	2,19%
Y	49	10,72%
Z	10	2,19%



Wir knacken Vigenère

Die Vigenère-Verschlüsselung wurde zum ersten Mal 1854 von dem englischen Mathematiker Charles Babbage (1792 - 1871) geknackt. Die meisten Wissenschaftler hatten zu diesem Zeitpunkt längst die Hoffnung aufgegeben.
Babbage ist vor allem für den ersten Entwurf eines modernen Computers bekannt. Um Vigenère zu brechen benutzte er aber keine Technik, sondern nur puren Scharfsinn. Wahrscheinlich wurde Babbage vom britischen Geheimdienst gezwungen, seine Entdeckung für sich zu behalten. Erst im 20. Jahrhundert fand man seine Arbeiten wieder.
Etwa neun Jahre nach Babbage fand auch der preußische Offizier Friedrich Wilhelm Kasiski (1805 - 1881) dieselbe Lösung des Problems. Da er das Verfahren sofort veröffentlichte, wird die folgende Methode auch als Kasiski-Test bezeichnet.

Babbage und Kasiski zerlegten das Problem in zwei Teile.

- Man muss herausfinden, wie lang das Schlüsselwort ist.
- Wenn man seine Länge kennt, muss das Schlüsselwort gefunden werden.

Als Beispiel nehmen wir uns noch einmal den längeren Geheimtext auf der letzten Seite vor, den wir ja bisher nicht entschlüsseln konnten.
Wir beginnen mit dem zweiten Teil der Lösung, da die ganze Sache dann leichter zu verstehen ist. Nehmen wir einmal an, dass der Geheimtext mit einem Schlüsselwort der Länge 3 geschrieben wurde. Dann ist jeder vierte Buchstabe des Textes mit demselben Ge- heimalphabet verschlüsselt worden. Wenn wir nun die Nachricht buchstabenweise auf die drei (uns noch unbekannten) Buchstaben des Schlüsselwortes verteilen, so erhält man:

Mit dem ersten Buchstaben des Schlüsselworts wurde verschlüsselt:

```
PPTLJUDKULLULHLVMSYAPYHULLDRKULUYLLHZBNAKMBLHOZLBLH
LJPTAKIKZVVPHQYNAIDKMPLINLSOKMLUAUKDUYJKIZBLYPTANLU
LZTOKTUKUUYHLUYLLZKZZSKUYZBLUHIJUHHSOYKKMPLHOPLLLBL
```

Mit dem zweiten Buchstaben des Schlüsselworts wurde verschlüsselt:

```
RRLYLEEVHFIWMVVPEPQWRJYHMRIMIHOHLWRIIRVIMVEVVVXJXVH
VLKYIIIIGRVREEIISIEMEPPXPGMYDVHQIEIIRRLMSIRHWIYIIWA
VMEXIEYHOHRWFDLPFSIEMEIISIRVSYVLHWIMISEMEPFYXQVYVV
```

Mit dem dritten Buchstaben des Schlüsselworts wurde verschlüsselt:

```
YYUMYGFUFNCNHGBTYYCYYLOMHTCHLCCYCMBHFXYFYUVQCYCGNXC
CNYNLLCHBPYJLBHMLHLYGCYYOEWHOCYCCHLHOCNYYTAYNZNLQYU
YYWYGHHYCYXFYOIFYHLFGHCAMBAMNMUOXNAWVNMYGCLWYGNLQX
```

Aufgaben:

- Führt für die Buchstaben eurer Gruppe eine Häufigkeitsanalyse durch und zeichnet für die relativen Häufigkeiten ein Balkendiagramm.
- Wie lautet also euer Buchstabe des Schlüsselworts?
- Entschlüsselt nun den Text eurer Gruppe vollständig. Denkt daran, dass es sich hier ja nur um eine ganz normale Caesar-Verschiebung handelt.
- Warum darf man innerhalb eurer Gruppe noch nicht damit rechnen, dass schon ein sinnvoller Text entstanden ist?
- Wenn ihr euch jetzt mit den anderen Gruppen austauscht, lässt sich das vollständige Schlüsselwort ermitteln. Wie lautet es?
- Setzt nun den Klartext im ständigen Wechsel mit den anderen Gruppen zusammen. Achtet auf euren Einsatz!

Wenn man also die Länge des Schlüsselworts schon kennt, ist es gar nicht mehr so schwer, die Vigenère-Verschlüsselung zu knacken. Wie aber kommt man zu dieser Länge?

Babbage und Kasiski fiel auf, dass es in den meisten Geheimtexten Wiederholungen gleicher Buchstabenfolgen gibt. Diese können rein zufällig entstanden sein, wenn sie aber ziemlich lang sind, ist das recht unwahrscheinlich. Was also könnte passiert sein? Nehmen wir uns dazu ein kleines Beispiel:

```
Schlüsselwort: MAUSMAUSMAUSMAUSMAUSMAUS
Klartext:      derhundderhirschdertiger
```

Hier taucht im Klartext dreimal das Wort „der" auf. Beim ersten und dritten Mal wird dieses Wort auf die gleiche Weise verschlüsselt, denn in beiden Fällen stehen über dem Wort „der" die Schlüsselwortbuchstaben M, A und U. Im zugehörigen Geheimtext werden sich also zwei gleiche Buchstabenfolgen wieder finden.
So etwas passiert immer dann, wenn der Abstand der gleichen Buchstabenfolgen ein Vielfaches der Schlüsselwortlänge ist. Oben beträgt die Länge des Schlüsselworts 4, der Abstand vom ersten „der" zum dritten „der" ist 16 (bitte nachzählen!) und 16 ist ja ein Vielfaches von 4.

Um nun die Länge des Schlüsselwortes zu ermitteln, geht man einfach so vor:

- Man sucht im Geheimtext nach gleichen Buchstabenfolgen. Sie sollten möglichst lang sein (mindestens 3 oder besser noch 4 gleiche Buchstaben hintereinander).
- Dann bestimmt man zu jeweils zwei gleichen Folgen ihren Abstand, der sehr wahrscheinlich ein Vielfaches der Schlüsselwortlänge ist.
- Zum Schluss berechnet man den größten gemeinsamen Teiler (ggT) dieser Abstände, höchstwahrscheinlich hat man dann die Schlüsselwortlänge gefunden. Da einzelne gleiche Buchstabenfolgen aber auch zufällig entstanden sein könnten, muss man hier leider mit Ausnahmen rechnen. Meistens funktioniert es aber.

Probieren wir das Ganze nun einfach an dem längeren Geheimtext von oben aus.
Wir wissen ja schon, dass die Länge des Schlüsselworts 3 ist. Liefert der gerade beschriebene Weg auch dieses Ergebnis?

PRYPRYTLULYMJLYUEGDEFKVUUHFLFNLICUWNL
MHHVGLVBVPTMEYSPYYQCAWYPRYYJLHYOUHMLM
HLRTDICRMHKILUHCLOCUHYYLCLWMLRBHIHZIF
BRXNVYAIFKMYMVUBEVLVQHVCOVYZXCLJGBXNL
VXHHCLVCJLNPKYTYNAILKILIICKIHZGBVRPVV
YPRJHELQEBYIHNIMASLIIHDEL
KMYMEGPPCLPYIXYNPOLGESMWOYHKDOMVCLHYU
QCAICUEHKILDIHUROYRCJLNKMYISYZITBRALH
YYWNPIZTYNAILNIQLWYUAULVYZMYTEWOXYKIG
TEHUYHKHYUOCUHYYRXHWFLFYUDOYLILPFLFYZ
SHKILZEFZMGSEHKICUIAYSMZIBBRALVMUSNHY
MIVUJLOUHXHWNHIASMWOIVYSNKEMKMYMEGPPC
LFLHYWOXYPQGLVNLYLLVQBVXL

Die drei Buchstabenfolgen YPRY, OCUHYY und FLFY tauchen hier doppelt auf.

Die Abstände sind 57, 240 und 12.

Der ggT dieser drei Zahlen ist tatsächlich 3, es klappt also.

Aufgaben:

1. Suche in dem Geheimtext oben nach weiteren sich wiederholenden Buchstabenfolgen und bestimme jeweils ihren Abstand. Kommt man auch mit diesen Abständen zur Schlüsselwortlänge 3 ?
2. Warum kann es auch passieren, dass man mit der Berechnung des ggT nur ein Vielfaches der Schlüsselwortlänge bestimmen kann? Gib ein Beispiel an.
3. Entschlüssele den Text rechts nach allen Regeln der Kunst. Einziger Tipp: Auch dieser Geheimtext wurde mit dem Vigenère-Verfahren verschlüsselt.

LSRXUIBSRHQLTBWXBHSOZDBDJI
IQSVOSYVSRSOWHSWZSMCUECNPT
WGWHIHWWISMCSQTHLDRISSVVSL
TWQHQLGWJINYTFJXBHTBHXSHTF
ICHWRVPJSWHSPJBKIFSINXSOKT
UICZETGWIGMRVVJBHWSVPIWQSL
PITISRSOWHAICGGWZMRVIGSVUW
RSIRVGKTWWIYIXBIVSLTWQHQLG
WJIOYHHYTTXTZRZORCRMTAICGG
WZMRVIGSVUWRSIRVGKTWWIBMRV
XPIGWOYUNYACIHSRKSVBCIRVXT

(aus: Beutelspacher, Mathe-Welt
Geheimschriften, S. 16.)

Auch die Vigenère-Verschlüsselung ist also zu knacken. Wenn man die Länge des Schlüsselworts ermitteln kann, hat man schon so gut wie gewonnen. Der Rest ist dann durch mehrere Häufigkeitsanalysen zu erledigen.
Das Verfahren von Babbage und Kasiski funktioniert nicht mehr, wenn man den Schlüssel genau so lang macht wie die Nachricht selbst. Außerdem wählt man für den Schlüssel eine rein zufällige Buchstabenkombination.
Mit solchen Zufallsschlüsseln wurde erstmals gegen Ende des Ersten Weltkriegs in der amerikanischen Armee gearbeitet. Weil man jeden Schlüssel nur ein einziges Mal verwendete, spricht man hier auch von einem „One time pad". Noch heute wird der „heiße Draht" zwischen dem russischen und dem amerikanischen Präsidenten über ein solches One time pad gesichert.
Man kann nun mathematisch beweisen, dass es unmöglich ist, einen mit einem One time pad verschlüsselten Text zu knacken. Dieses Verschlüsselungssystem ist also nicht nur ziemlich, sondern wirklich absolut sicher, es ist die Krönung der Kryptographie.
In der Praxis ist es allerdings gar nicht so einfach, wirklich zufällige Schlüssel zu er- zeugen und an die Sender und Empfänger zu verteilen. Das aber ist ein ganz neues Thema.

Gruppenarbeit Vigenère

Wir bearbeiten den Text, der mit dem

1 ersten

1 zweiten

1 dritten

Buchstaben des Schlüsselworts verschlüsselt wurde.

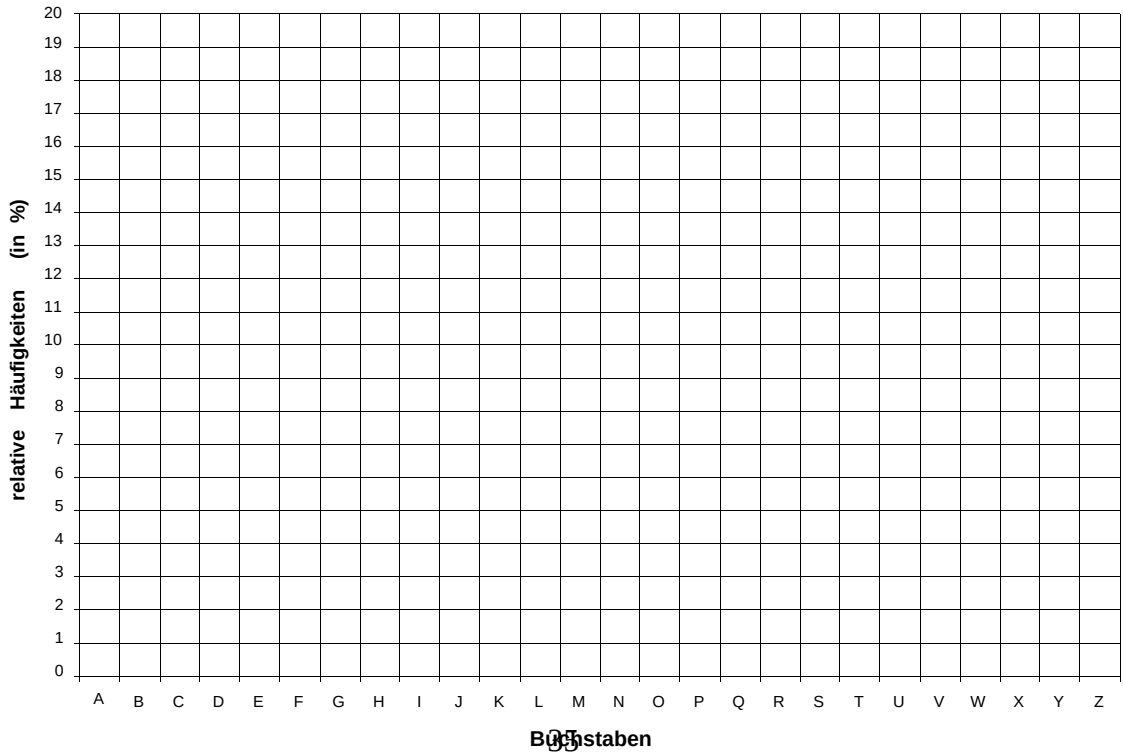
Ergebnis:

Der Klartextbuchstabe e steht für den Geheimtextbuchstaben: _____

Unser Buchstabe des Schlüsselworts ist also: _____

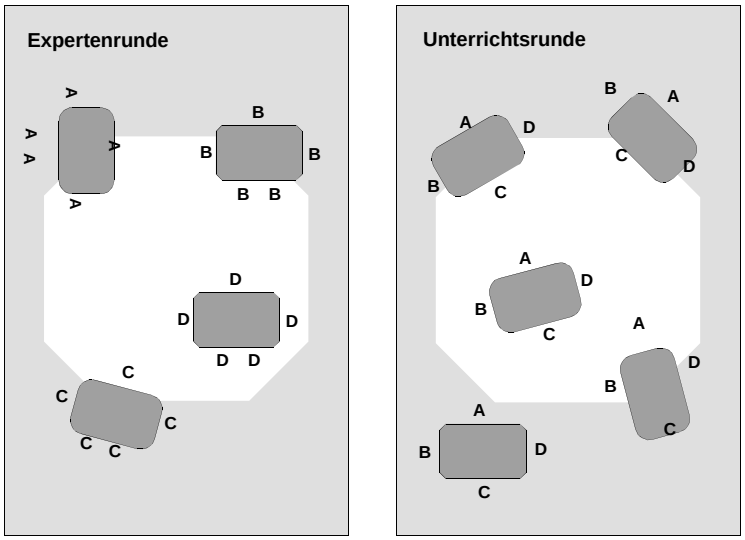
	Häufigkeitsanalyse		
Buchstabe	Strichliste	absolute Häufigkeit	relative Häufigkeit
A			
B			
C			
D			
E			
F			
G			
H			
I			
J			
K			
L			
M			
N			
O			
P			
Q			
R			
S			
T			
U			
V			
W			
X			
Y			
Z			

Balkendiagramm



Methode Jigsaw/Gruppenpuzzle

Die Methode Jigsaw („Laubsäge") trägt ihren Namen, weil eine größere Thematik in mehrere Teile „zersägt" wird. Diese Puzzlestücke werden an Gruppen verteilt und dort bearbeitet (Expertenrunde), bevor sie ebenfalls in Grup- penarbeit wieder zu einem Ganzen zusammen gefügt werden (Unterrichtsrunde).



Verwirbelung mit Methode: Expertengruppen teilen sich nach einer Einarbeitungsphase auf mehrere Unterrichtsgruppen auf und tragen ihr Wissen zusammen.

Expertenrunde:
Jeder Schüler/jede Schülerin bearbeitet die Aufgabenstellung.
Die Gruppenmitglieder vergleichen ihre Lösungen und klären Probleme.
Sie bereiten sich gemeinsam auf die 2. Runde vor, indem sie sich z. B. überlegen, wie das erarbeitete Wissen den Mitschülerinnen und Mitschülern vermittelt werden soll oder was diese in ihr Heft notieren sollen. Auch überlegen sie sich Kontrollfragen, legen Übungsaufgaben fest, bilden ähnliche neue Aufgaben, entscheiden sich für notwendige Hausaufgaben, erstellen ein Lernplakat, etc.
Jeder Schüler dieser ersten Gruppe ist jetzt für sein Gebiet/seinen Aufgabentyp der Experte.

Unterrichtsrunde:
Es werden neue Gruppen gebildet.
In jeder Gruppe ist pro Gebiet/pro Aufgabentyp ein Experte vorhanden, der nun den anderen Tischgruppenmitgliedern sein Wissen vermittelt, Erklärungen gibt, ihnen Kontrollfragen und Aufgaben stellt, diese kontrolliert und dafür verantwortlich ist, dass die Gruppenmitglieder lernen.

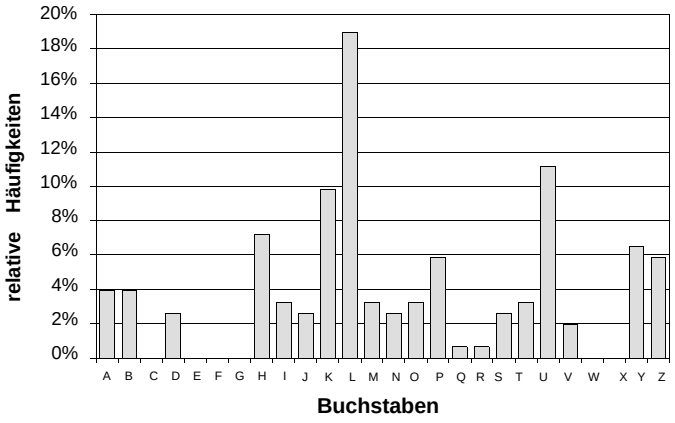
Beispiel zum Einsatz dieser Methode:

Die drei Geheimtexte, die mit jeweils einem Buchstaben des Schlüsselworts verschlüsselt wurden, werden auf die Expertenrunden aufgeteilt. Jede Expertenrunde führt nun für ihren Text auf dem Arbeitsblatt eine Häufigkeitsanalyse durch, zeichnet ein Balkendiagramm für die relativen Häufigkeiten, bestimmt den zugehörigen Buchstaben des Schlüsselworts und entschlüsselt schließlich den vollständigen Text.
In der sich anschließenden Unterrichtsrunde stellen die Experten ihre Ergebnisse kurz dar und setzen zunächst das Schlüsselwort sowie danach auch den voll- ständigen Klartext aus den bereits entschlüsselten Teiltexten reihum zusammen.

Wir knacken Vigenère - Lösungen zur Gruppenarbeit

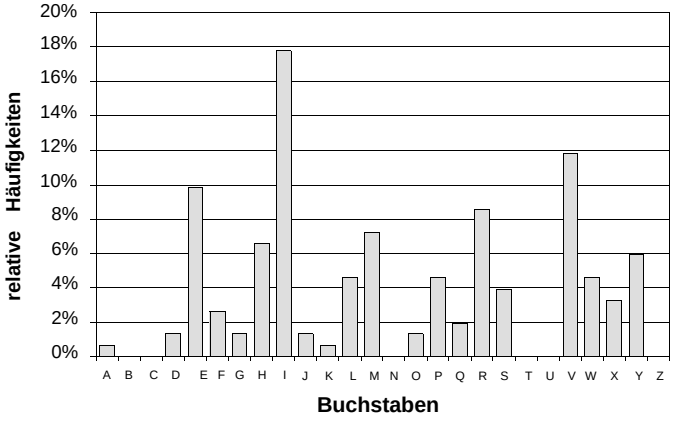
Geheimtext-buchstabe	absolute Häufigkeit	relative Häufigkeit	Klartext-buchstabe
A	6	3,92%	t
B	6	3,92%	u
C	0	0,00%	v
D	4	2,61%	w
E	0	0,00%	x
F	0	0,00%	y
G	0	0,00%	z
H	11	7,19%	a
I	5	3,27%	b
J	4	2,61%	c
K	15	9,80%	d
L	29	18,95%	e
M	5	3,27%	f
N	4	2,61%	g
O	5	3,27%	h
P	9	5,88%	i
Q	1	0,65%	j
R	1	0,65%	k
S	4	2,61%	l
T	5	3,27%	m
U	17	11,11%	n
V	3	1,96%	o
W	0	0,00%	p
X	0	0,00%	q
Y	10	6,54%	r
Z	9	5,88%	s

Gruppe 1: erster Schlüsselwortbuchstabe



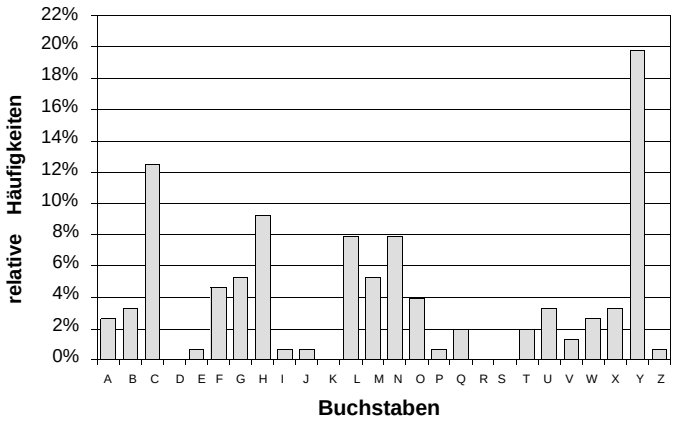
Geheimtext-buchstabe	absolute Häufigkeit	relative Häufigkeit	Klartext-buchstabe
A	1	0,66%	w
B	0	0,00%	x
C	0	0,00%	y
D	2	1,32%	z
E	15	9,87%	a
F	4	2,63%	b
G	2	1,32%	c
H	10	6,58%	d
I	27	17,76%	e
J	2	1,32%	f
K	1	0,66%	g
L	7	4,61%	h
M	11	7,24%	i
N	0	0,00%	j
O	2	1,32%	k
P	7	4,61%	l
Q	3	1,97%	m
R	13	8,55%	n
S	6	3,95%	o
T	0	0,00%	p
U	0	0,00%	q
V	18	11,84%	r
W	7	4,61%	s
X	5	3,29%	t
Y	9	5,92%	u
Z	0	0,00%	v

Gruppe 2: zweiter Schlüsselwortbuchstabe



Geheimtext-buchstabe	absolute Häufigkeit	relative Häufigkeit	Klartext-buchstabe
A	4	2,63%	g
B	5	3,29%	h
C	19	12,50%	i
D	0	0,00%	j
E	1	0,66%	k
F	7	4,61%	l
G	8	5,26%	m
H	14	9,21%	n
I	1	0,66%	o
J	1	0,66%	p
K	0	0,00%	q
L	12	7,89%	r
M	8	5,26%	s
N	12	7,89%	t
O	6	3,95%	u
P	1	0,66%	v
Q	3	1,97%	w
R	0	0,00%	x
S	0	0,00%	y
T	3	1,97%	z
U	5	3,29%	a
V	2	1,32%	b
W	4	2,63%	c
X	5	3,29%	d
Y	30	19,74%	e
Z	1	0,66%	f

Gruppe 3: dritter Schlüsselwortbuchstabe



Die normale Häufigkeitsverteilung der Buchstaben bleibt bei Caesar-Verschiebungen erhalten, sie ist nur verschoben. An den Balkendiagrammen lassen sich daher die charakteristischen Merkmale der Häufigkeitsverteilung schnell wieder finden. Eine Zuordnung der Klartextbuchstaben bereitet so überhaupt keine Schwierigkeiten.

Das gesuchte Schlüsselwort ist HEU.

Als Klartext ergibt sich der Beginn des Märchens „Hänsel und Gretel":

```
ineinemhaeuschenamwaldrandlebteeinste
inarmerholzfaellermitseinerfrauundsei
nenzweikinderndiekinderhiessenhaensel
undgreteldiefrauaberwarihrestiefmutte
rdadierichtigemutterderbeidenschonvor
einpaarjahrengestorbenwar
diefamilielebtegluecklichundzufrieden
miteinanderwennnurnichtdieboesezunged
erstiefmuttergewesenwaeresiemachtedem
mannunddenkinderndaslebenzurhoellebes
ondersalsimlandeinegrossehungersnotau
sbrachunddastaeglichebrotdasdiefamili
ebrauchteimmerteurerwurde
```